UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

Resolución: **RPC-SO-02-No.053-2021**

PROYECTO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGÍSTER

Título del proyecto:
CONSIDERACIONES PARA LA IMPLEMENTACIÓN DEL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA LEY DE PROTECCIÓN DE DATOS PERSONALES CASO DE ESTUDIO: INSTITUTO NACIONAL DE PATRIMONIO CULTURAL
Línea de Investigación:
Seguridad Informática
Campo amplio de conocimiento:
Tecnología de la Información y Comunicaciones
Autor:
Jorge Luis Jaramillo Burbano
Tutor:
Mg. Christian Patricio Vaca Benalcázar CPA

Quito – Ecuador

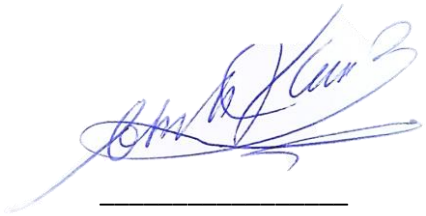
2022

APROBACIÓN DEL TUTOR

Yo, Christian Vaca con C.I: 1719368555 en mi calidad de Tutor del proyecto de investigación titulado: “Consideraciones Para La Implementación Del Esquema Gubernamental De Seguridad De La Información Basado En La Ley De Protección De Datos Personales Caso De Estudio: Instituto Nacional De Patrimonio Cultural.”

Elaborado por: Jorge Luis Jaramillo Burbano, de C.I: 1713677902, estudiante de la Maestría: Maestría en Seguridad Informática, de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., septiembre de 2022



_____

Firma

Tabla de contenido

APROBACIÓN DEL TUTOR 2
INFORMACIÓN GENERAL 1
Contextualización del tema 1
Problema de investigación 1
Objetivo general 1
Objetivos específicos 1
Vinculación con la sociedad y beneficiarios directos: 2
CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO 3
1.1. Contextualización general del estado del arte 3
1.2. Proceso investigativo metodológico 3
1.3. Análisis de resultados 3
CAPÍTULO II: PROPUESTA 11
1.1. Fundamentos teóricos aplicados 11
1.2. Descripción de la propuesta 13
1.3. Validación de la propuesta 32
CONCLUSIONES 33
RECOMENDACIONES 34
BIBLIOGRAFÍA 35
ANEXOS 37

Índice de tablas

Tabla 1 Parámetros de la encuesta. 4
Tabla 2 Escalas de Valoración 5
Tabla 3 Nivel de Conocimiento por Secciones de la encuesta 10
Tabla 4 Normativa Datos Personales Chile, Ecuador, Perú 14
Tabla 5 Concordancia LOPDP Ecuador - Reglamento Perú 15
Tabla 6 Controles EGSI V2 con Artículos LOPD 18
Tabla 7 Consideraciones para cumplimiento de la LOPDP 19

Índice de figuras

Figura 1 Número de Encuestas Realizadas 4
Figura 2 Envío de correo con encuesta 5
Figura 3 Resultados Pregunta 1 5
Figura 4 Resultados Pregunta 2 6
Figura 5 Resultados Pregunta 3 6
Figura 6 Resultados Pregunta 4 6
Figura 7 Resultados Pregunta 5 7
Figura 8 Resultados Pregunta 6 7
Figura 9 Resultados Pregunta 7 8
Figura 10 Resultados Pregunta 8 8
Figura 11 Estructura General de la Propuesta 28

INFORMACIÓN GENERAL

Contextualización del tema

Con el gran avance de la tecnología y la utilización de esta en todos los ámbitos, conscientes de las amenazas y riesgos a los que se está expuesto en el día a día, varias instituciones públicas y privadas han generado directrices, buenas prácticas, metodologías, leyes, políticas y normativa para controlar esta problemática. (Gascó, 2013)

A nivel de Gobierno, la seguridad de la información y tratamiento de datos personales se convierte con el tiempo en una premisa que debe ser tratada con la importancia que esta demanda.

Problema de investigación

¿Qué criterios se deben aplicar en la implementación del Esquema Gubernamental de Seguridad de la Información para cumplir con lo establecido por la Ley Orgánica de Protección de Datos Personales (LOPDP) en el Instituto Nacional de Patrimonio Cultural (INPC)?

Objetivo general

Proponer un procedimiento interno en el Instituto Nacional de Patrimonio Cultural, para que los controles definidos en el Esquema de Seguridad de la Información (EGSI) cumplan con los artículos de la Ley Orgánica de Datos Personales que sean aplicables para la institución, mediante un análisis situacional que mitigue el riesgo de pérdida de información.

Objetivos específicos

1. Revisar la literatura relacionada con la legislación para protección de datos personales, para documentar los aspectos más relevantes de estos marcos regulatorios.
2. Identificar los aspectos que cubre el Reglamento de la Ley Nº 29733 - Ley de Protección de Datos Personales de Perú, para tener una línea base mientras se emite el reglamento en Ecuador.
3. Evaluar mediante una encuesta el nivel de conocimiento que tiene el personal del INPC referente a la normativa de seguridad de la información.
4. Proponer las consideraciones técnicas que permitan relacionar los controles del EGSI con la Ley Orgánica de Protección de Datos Personales.
5. Facilitar lineamientos para proteger los datos personales e información sensible del patrimonio cultural del Ecuador, puesto que la cultura desempeña un papel fundamental en el logro del Objetivo de Desarrollo Sostenible 11, que su propósito es la protección y salvaguarda del patrimonio natural y cultural del mundo.

Vinculación con la sociedad y beneficiarios directos:

El presente trabajo de investigación se realizó en el Instituto Nacional de Patrimonio Cultural que su principal actividad es promover, difundir y gestionar la preservación, conservación y salvaguardia del patrimonio cultural material e inmaterial, mediante la investigación y el control técnico conforme a las políticas públicas emitidas por el ente rector.

El INPC tiene una vinculación directa con la ciudadanía en general ya que brinda servicios públicos como: Autorización de Movilización de Bienes Culturales, Registro de Profesionales, Servicios Especializados de Laboratorio, administra el Sistema de Información del Patrimonio Cultural, entre otros, todos estos servicios recopilan información y datos personales.

El INPC contribuye en gran parte a la reactivación económica del sector cultural, con estímulos directos hacia investigadores, gestores culturales, portadores de saberes del patrimonio cultural.

Mediante las consideraciones que se emitan en este documento se podrá llegar a obtener procesos de manejo de la información y tratamiento de datos personales más seguros a nivel gubernamental, lo que contribuirá en el aumento de confianza del manejo de información en sistemas de información gubernamentales.

CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO

1.1. Contextualización general del estado del arte

Con el gran avance de la tecnología y la utilización de esta en todos los ámbitos, conscientes de las amenazas y riesgos a los que se está expuesto en el día a día, varias instituciones públicas y privadas han generado directrices, buenas prácticas, metodologías, leyes, políticas y normativa para controlar esta problemática.

A nivel de Gobierno, la seguridad de la información y tratamiento de datos personales se convierte con el tiempo en una premisa que debe ser tratada con la importancia que esta demanda. (Gascó, 2013)

1.2. Proceso investigativo metodológico

Enfoque de Investigación

Se empleó un enfoque cuantitativo con un alcance no experimental transversal, además se aplicó un método de encuesta mediante Google Formularios como técnica para la recopilación de datos existentes

Población y Muestra

Se utilizó un muestreo No Probabilístico por cuotas, ya que se conformó grupos tomados de la población de acuerdo al criterio del investigador.

El universo que se aplicó la encuesta fue de 150 personas a nivel nacional, entre funcionarios técnicos y nivel jerárquico superior, que son funcionarios que en sus actividades diarias utilizan o generan información con algún nivel de tratamiento de datos personales.

1.3. Análisis de resultados

Se elaboró una encuesta para medir el conocimiento de los funcionarios sobre Seguridad de la Información, EGSI y LOPDP, la encuesta consta de ocho preguntas distribuidas de la siguiente manera:

- Dos preguntas sobre Seguridad Informática.
- Dos preguntas sobre EGSI.
- Cuatro preguntas sobre Ley Orgánica de Protección de Datos Personales.

Las preguntas se elaboraron considerando que el tratamiento de datos personales es un tema nuevo en el país y fue publicado en la LOPDP en mayo del 2021. Además, se tomó en cuenta que actualmente la seguridad de la información ha tenido un repunte por la gran cantidad de ataques cibernéticos que son de dominio público pero que a su vez son temas

técnicos que poca gente conoce como se aplica, lo que podría ocasionar que los encuestados no den respuestas totalmente confiables.

Las preguntas 1, 2, 3, 4, 5, 7, 8 son de tipo cerradas con una sola respuesta correcta y la pregunta 8 es de casillas de verificación con dos respuestas correctas.

Para la realización de la encuesta ha tomado en cuenta los siguientes parámetros:

Tabla 1

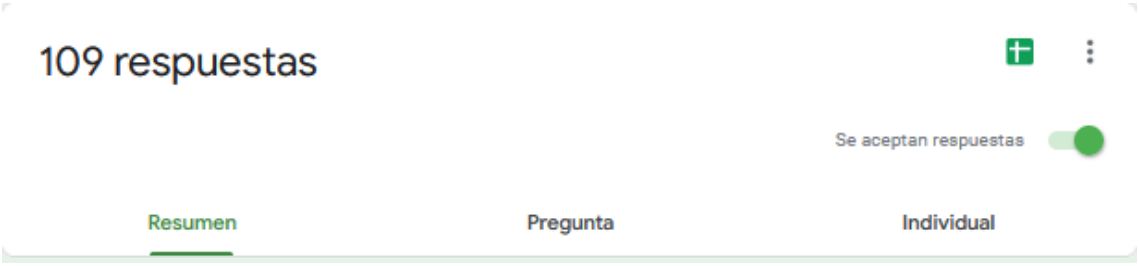
Parámetros de la encuesta.

Parámetros	Valores
Tamaño del universo	150 personas
Heterogeneidad	50 %
Margen de Error	5
Nivel de Confianza	95
Muestra	109

Nota. Esta tabla indica los parámetros que se utilizaron para realizar la encuesta a los funcionarios del INPC.

Figura 1

Número de Encuestas Realizadas



Nota. La figura indica en número de funcionarios del INPC que fueron encuestados a nivel nacional.

En el Anexo 1 del trabajo de investigación se encuentra la plantilla de las preguntas utilizadas en la encuesta.

La tabulación de los resultados de las preguntas realizadas presenta un nivel de conocimiento categorizado según el tema, se detalla a continuación:

Tabla 2

Escalas de Valoración

Porcentaje	Valoración
0% - 20%	Nulo
21% - 40%	Bajo
41% - 60%	Medio
61% - 80%	Alto
81% - 100%	Avanzado

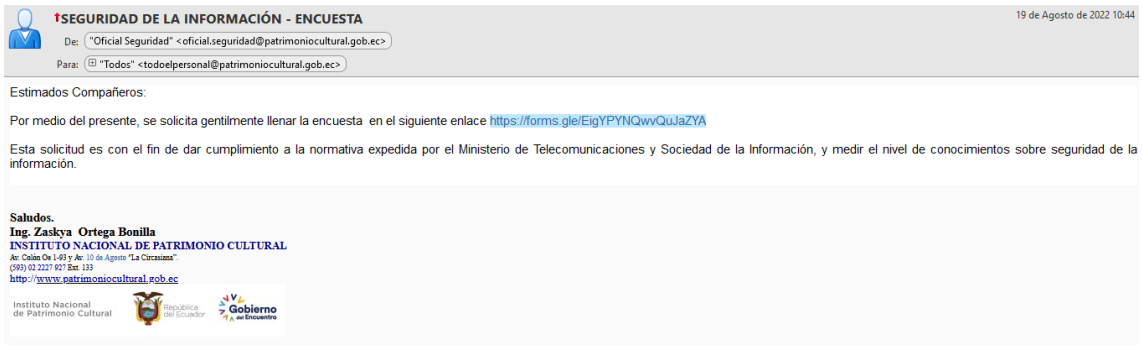
Nota. La tabla indica el porcentaje y valoración del nivel de conocimiento de los encuestados.

La encuesta se elaboró en la herramienta de Google Formularios.

El envío de la encuesta se realizó mediante correo electrónico institucional, remitido desde la cuenta del Oficial de Seguridad de la institución.

Figura 2

Envío de correo con encuesta



Nota. Captura de pantalla del correo electrónico enviado a los funcionarios del INPC para que realicen la encuesta.

A continuación, se muestra los resultados por número de pregunta:

Figura 3

Resultados Pregunta 1

Nota. La figura presenta los porcentajes de los resultados obtenidos en la pregunta 1.

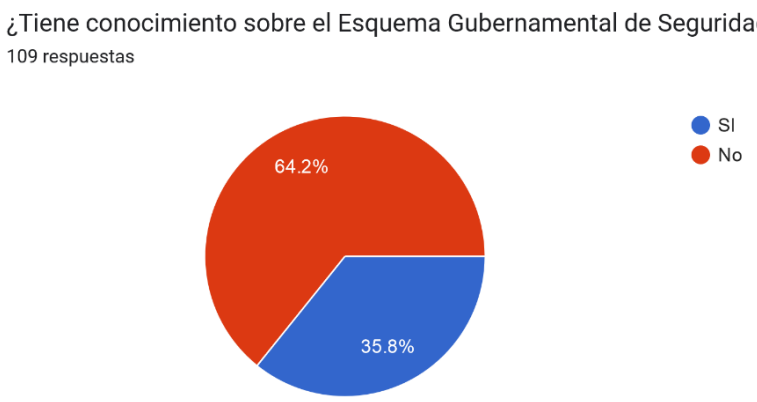
Figura 4

Resultados Pregunta 2

Nota. La figura presenta los porcentajes de los resultados obtenidos en la pregunta 2.

Figura 5

Resultados Pregunta 3



Nota. La figura presenta los porcentajes de los resultados obtenidos en la pregunta 3.

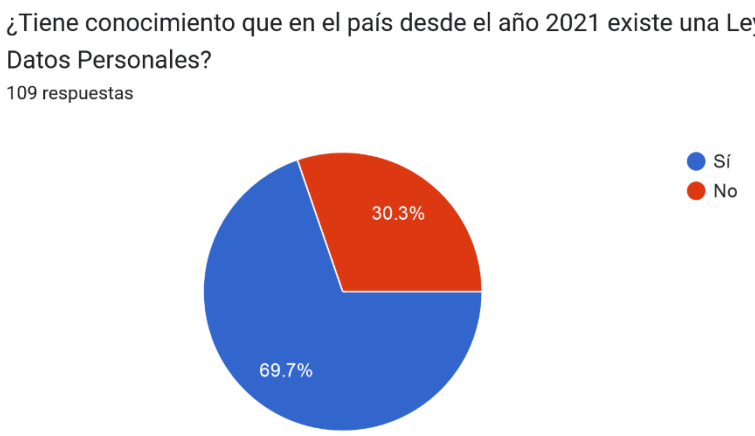
Figura 6

Resultados Pregunta 4

Nota. La figura presenta los porcentajes de los resultados obtenidos en la pregunta 4.

Figura 7

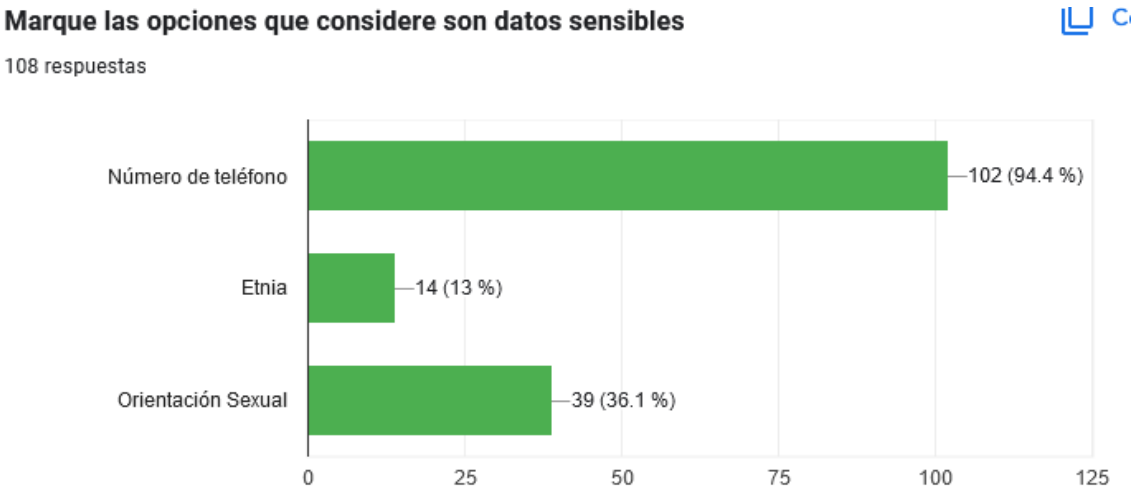
Resultados Pregunta 5



Nota. La figura presenta los porcentajes de los resultados obtenidos en la pregunta 5

Figura 8

Resultados Pregunta 6



Nota. La figura presenta los porcentajes de los resultados obtenidos en la pregunta 6 , en la cual se puede verificar que la mayoría de encuestados respondieron erróneamente.

Figura 9

Resultados Pregunta 7

Nota. La figura presenta los porcentajes de los resultados obtenidos en la pregunta 7.

Figura 10

Resultados Pregunta 8

Nota. La figura presenta los porcentajes de los resultados obtenidos en la pregunta 8.

De la tabulación realizada se desprenden los siguientes datos:

Tabla 3

Nivel de Conocimiento por Secciones de la encuesta

Sección	Porcentaje	Nivel
I Seguridad de La Información	94,5	Avanzado
II EGSI	61,45	Alto
III LOPDP	52,1	Medio

Nota. Esta tabla muestra la clasificación obtenida según los porcentajes de las respuestas de la encuesta.

El nivel de conocimiento sobre la Ley Orgánica de Protección de Datos Personales es el más bajo con un porcentaje de 52,1 %.

CAPÍTULO II: PROPUESTA

1.1. Fundamentos teóricos aplicados

A continuación, se describen varios conceptos, normativas y leyes como: Ciberseguridad, Seguridad de la Información, Tratamiento de Datos Personales, Ley Orgánica de Protección de Personales, Esquema Gubernamental de Seguridad de la Información y Estatuto Orgánico del Instituto Nacional de Patrimonio Cultural, los mismos que son fundamentales y formarán parte del objeto de estudio de este proyecto de investigación.

Ciberseguridad

"Protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados". (Corletti, 2017)

Seguridad de la Información

"La seguridad de la información es el conjunto de medidas y procedimientos, tanto humanos como técnicos, que permiten proteger la integridad, confidencialidad y disponibilidad de la información. Integridad: certificando que tanto la información como sus métodos de proceso son exactos y completos; confidencialidad: asegurando que únicamente pueden acceder a la información y modificarla los usuarios autorizados; disponibilidad: permitiendo que la información esté disponible cuando los usuarios la necesiten. Este término, por tanto, es un concepto amplio que engloba medidas de seguridad que afectan a la información independientemente del tipo de esta, soporte en el que se almacene, forma en que se transmita, etc." (Gascó, 2013)

Tratamiento de datos personales

El Ministerio de Telecomunicaciones y de la Sociedad de la Información establece una política y guía para el tratamiento de datos personales, donde se menciona que: "El tratamiento de datos personales en la Administración Pública Central, tiene por objeto proporcionar lineamientos para que las entidades de la Administración Pública Central (APC) mantengan informadas a las personas que acceden a través de sus canales electrónicos, sobre el tratamiento que dan a sus datos personales; y gestionen de manera adecuada los datos personales" (Guía para Tratamiento de Datos Personales en Administración Pública, 2019).

Constitución de la República del Ecuador

Publicada en octubre de 2008, y con su última modificación realizada el 25 de enero de 2021. Es la Norma Suprema bajo la que está sometida toda la legislación ecuatoriana, aquí se establecen todas las normas fundamentales que amparan los derechos obligaciones y libertades de los ciudadanos y del Estado.

Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos

Por el avance de la utilización de sistemas de información y redes electrónicas de datos incluida la Internet, se requiere normar, regular y controlar el uso de las relaciones económicas y de comercio mediante esta Ley especializada que fue publicada el 10 de abril de 2002.

Ley Orgánica de Protección de Personales

La finalidad de esta ley es garantizar el derecho a la protección de datos personales, incluido el acceso y decisión sobre la información y datos de este tipo, también su correspondiente protección y está conformada por 12 capítulos: Capítulo I: Ámbito de Aplicación Integral; Capítulo II: Principios; Capítulo III: Derechos; Capítulo IV: Categorías Especiales de Datos; Capítulo V: Transferencia o Comunicación y Acceso a Datos Personales por Terceros; Capítulo VI: Seguridad de Datos Personales; Capítulo VII: Del Responsable y del Delegado de Protección de Datos Personales; Capítulo VIII: De la Responsabilidad Proactiva; Capítulo IX: Transferencia o Comunicación Internacional de Datos Personales; Capítulo X: De los Requerimientos Directos y de la Gestión del Procedimiento Administrativo; Capítulo XI: Medidas Correctivas, Infracciones y Régimen Sancionatorio; Capítulo XII: Autoridad de Protección de Datos Personales.

Esquema gubernamental de Seguridad de la Información

A finales del 2013, el Ministerio de Telecomunicaciones y Sociedad de la Información expidió el Esquema Gubernamental de Seguridad de la Información (EGSI) mediante el acuerdo ministerial 166. El EGSI está elaborado en base a las NTE-INEN ISO/IEC 27001, NTE-INEN ISO/IEC 27002 y NTE-INEN ISO/IEC 27005.

Este sistema engloba los activos de la información que soportan los procesos de gestión que se desarrollan en INPC. El alcance del Esquema Gubernamental de Seguridad de la Información es para: "La protección de todos los activos de información y datos del Inventario de Bienes Culturales Patrimoniales que permiten el desempeño normal y exitoso de las funciones, servicios y actividades del Instituto Nacional de Patrimonio Cultural".

Estatuto Orgánico del Instituto Nacional de Patrimonio Cultural

Para complementar la investigación es importante conocer el Estatuto Orgánico de Gestión Organizacional por Procesos del INPC, ya que ayudará a comprender cómo fluye la información en las diferentes áreas y determinar amenazas y vulnerabilidades que pueden ser explotadas.

"Los procesos que elaboran los productos y servicios del Instituto Nacional de Patrimonio Cultural, INPC, se ordenan y clasifican en función de su grado de contribución o valor agregado al cumplimiento de la misión institucional" (Estatuto Orgánico de Gestión Organizacional por Procesos del Instituto Nacional de Patrimonio Cultural, 2011).

Reglamento de la Ley N 29733, Ley de Protección de Datos Personales

Para el presente trabajo de investigación, considerando que en Ecuador no existe todavía un Reglamento de la Ley Orgánica de Datos Personales, se ha tomado como referencia el Reglamento de la Ley N 29733, Ley de Protección de Datos Personales de Perú expedida el 22 de marzo de 2013, ya que es uno de los países de América Latina que ha implementado normativa sobre protección de datos personales.

1.2. Descripción de la propuesta

El estudio presenta las consideraciones necesarias para la implementación de un esquema de seguridad de la información basado en la LOPDP para el INPC, mediante el análisis de la normativa vigente para generar un proceso interno que permita el cumplimiento de los controles y artículos definidos en el EGSI y la LOPDP.

Análisis de Normativa Vigente

Tiene por objetivo la revisión sistémica de los reglamentos a la Ley de Protección de Datos Personales de los países de Perú y Chile, para escoger un reglamento que pueda ser aplicado a la LOPDP del Ecuador.

En el Ecuador la LOPDP fue publicada en mayo del año 2021, pero hasta el momento no existe un Reglamento a esta ley por lo que, para poder realizar el trabajo de investigación denominado: "CONSIDERACIONES PARA LA IMPLEMENTACIÓN DEL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA LEY DE PROTECCIÓN DE DATOS PERSONALES CASO DE ESTUDIO: INSTITUTO NACIONAL DE PATRIMONIO CULTURAL", es necesario tener una normativa que regule la aplicación de la ley, en este caso se realizará un análisis sistémico entre los reglamentos de Chile y Perú, mismos que están basados en el Reglamento de Protección de Datos Personales de la Unión Europea y que Ecuador también está trabajando sobre este para

generar el Reglamento. Se ha tomado como referencia estos dos países ya que se encuentran en la región.

Tabla 4

Normativa Datos Personales Chile, Ecuador, Perú.

PAÍS	Ley Orgánica de Protección de Datos Personales	Reglamento a la Ley Orgánica de Protección de Datos Personales
CHILE	LEY N° 19.628: PROTECCIÓN DE DATOS PERSONALES	Decreto 779 APRUEBA REGLAMENTO DEL REGISTRO DE BANCOS DE DATOS PERSONALES A CARGO DE ORGANISMOS PUBLICOS
ECUADOR	Ley Orgánica de Protección de Datos Personales	NO EXISTE
PERÚ	Ley Nº 29733, Ley de Protección de Datos Personales	Reglamento a la Ley Nº 29733, Ley de Protección de Datos Personales

Nota. La tabla muestra la normativa que fue analizada para realizar el presente trabajo

Se ha seleccionado a dos países de la región que tienen una larga trayectoria en la implementación de normativa para el tratamiento de datos personales como son: Chile quien ha trabajado en protección de datos desde 1999, año que promulgó su primera ley sobre el tema; y Perú que desde el 2011 ha venido desarrollando normativa sobre protección de datos personales, misma que no ha sufrido cambios en los últimos años.

Además, se tomó en cuenta la normativa de Perú para realizar la comparación porque los factores culturales, sociales y económicos son similares a nivel de Latinoamérica, lo que favoreció esta investigación.

Observación:

La Ley N° 19.628: Protección De Datos Personales de Chile se encuentra actualmente en una propuesta de modificación.

Una vez que se realizó la revisión de la normativa sobre protección de datos personales de los países de Chile y Perú, se ha tomado como decisión realizar el trabajo de investigación basado en el Reglamento de Protección de Datos Personales de Perú, por motivo que la normativa de Chile está en proyecto de modificación mismo que fue aprobado el 2 de junio de 2022, mientras que la normativa peruana no tiene proyectos de cambios.

Revisión Sistémica entre EGSI, LOPDP y Reglamento a la Ley (Perú)

En el documento ANEXO 2, se realiza una concordancia entre los artículos de la Ley Orgánica de Protección de Datos Personales que son aplicables en el instituto de investigación y el Reglamento a la Ley Nº 29733, Ley de Protección de Datos Personales del Perú.

Para saber que artículos de la LOPDP deben cumplirse obligatoriamente en el INPC se ha tomado en cuenta tratamiento de datos, la información recopilada por diferentes medios en la institución, la misión y visión institucional.

En la siguiente tabla se puede visualizar un resumen del reglamento del Perú que se puede considerar como una buena práctica para la normativa ecuatoriana.

Tabla 5

Concordancia LOPDP Ecuador - Reglamento Perú

LOPDP	**Reglamento de la ley No 29733, Ley de Protección de Datos Personales**
Art. 7.- Tratamiento legítimo de datos personas	Capítulo I Consentimiento Artículos 11, 12, 13, 14, 15, 16.
Art. 8.- Consentimiento. -	Capítulo I Consentimiento Artículos 11, 12, 13, 14, 15, 16. Capítulo II Limitaciones al consentimiento Artículo 17.
Art. 9.- Interés legítimo	Artículo 8.- Principio de finalidad
Art. 10.- Principios	TÍTULO II Principios rectores art. 6 al 10
Art. 11.- Normativa especializada	No existe articulo Similar
Art. 12.- Derecho a la información	Artículo 60
Art. 13.- Derecho de acceso	Articulo 61
Art. 14.- Derecho de rectificación y actualización	Artículos 64, 65
Art. 15.- Derecho de eliminación	Artículos 67, 68, 69,70
Art. 16.- Derecho de oposición	Artículo. 71
Art. 17.- Derecho a la portabilidad	Artículo 33
Art. 18.- Excepciones a los derechos de rectificación, actualización, eliminación, oposición, anulación y portabilidad	Artículo 59
Art. 19.- Derecho a la suspensión del tratamiento	Artículo 67
Art. 25.- Categorías especiales de datos personales	Capitulo IV tratamientos especiales de datos personales, artículo 27
Art. 26.- Tratamiento de datos sensibles	Artículo 14

LOPDP	**Reglamento de la ley No 29733, Ley de Protección de Datos Personales**
Art. 27.- Datos personales de personas fallecidas	Al respecto, debemos manifestar que la Ley N° 29733, Ley de Protección de Datos Personales (en adelante, "LPDP"), define al titular de datos personales como la "persona natural a quien corresponde los datos personales". En tal sentido, habiendo señalado que la muerte le pone fin a la persona y considerando que la mencionada ley sólo tutela los datos personales de las personas naturales, resulta evidente que el derecho a la protección de datos personales desaparece por la muerte, por lo que los tratamientos de datos de personas fallecidas no podrían considerarse comprendidos dentro del ámbito de aplicación de la LPDP.
Art. 33.- Transferencia o comunicación de datos personales	Artículo 18
Art. 34.- Acceso a datos personales por parte del encargado	Artículo 36
Art. 35.- Acceso a datos personales por parte de terceros	Artículos 37 y 38
Art. 36.- Excepciones de consentimiento para la transferencia o comunicación de datos personales	Capítulo II Limitaciones al consentimiento Artículo 17
Art. 37.- Seguridad de datos personales	Capítulo V Medidas de Seguridad Medidas de seguridad artículo 39
Art. 38.- Medidas de seguridad en el ámbito del sector público	La normativa no diferencia el sector público y el sector privado
Art. 39.- Protección de datos personales desde el diseño y por defecto	Artículo 39
Art. 40.- Análisis de riesgo, amenazas y vulnerabilidades	Artículo 40
Art. 41.- Determinación de medidas de seguridad aplicables	Artículo 40
Art. 43.- Notificación de vulneración de seguridad	Artículo 40
Art. 46.- Notificación de vulneración de seguridad al titular	Artículo 40

LOPDP	Reglamento de la ley No 29733, Ley de Protección de Datos Personales
Art. 55.- Transferencia o comunicación internacional de datos personales	Artículos 24,25,26
Art. 56.- Transferencia o comunicación internacional de datos personales a países declarados como nivel adecuado de protección	Artículos 24,25,26
Art. 57.- Transferencia o comunicación mediante garantías adecuadas	Artículos 24,25,26
Art. 59.- Autorización para transferencia internacional	Artículos 24,25,26
Art. 60.- Casos excepcionales de transferencias o comunicaciones internacionales	Artículos 24,25,26
Art. 61.- Control continuo	Artículo 75
Artículo 63 Actuaciones Previas Artículo 64 Procedimiento administrativo	Título 4 Capítulo I Disposiciones Generales Artículos 47,48,49, 50, 51, 52, 53,54, 55, 56, 57, 58, 59
Art. 62.- Requerimiento directo del titular del dato de carácter personal al responsable del tratamiento	Título 4 Capítulo I Disposiciones Generales Artículos 47,48,49, 50, 51, 52, 53,54, 55, 56, 57, 58, 59

Nota. La tabla muestra la concordancia entre los artículos de la LOPDP de Ecuador con el Reglamento de la ley No 29733, Ley de Protección de Datos Personales del Perú

Emparejamiento de Controles del EGSI con la LOPDP

Para realizar este análisis entre los controles se Seguridad de la Información EGSI versión 2 y los artículos de la Ley Orgánica de Protección de Datos Personales que deben ser cumplidas en el INPC, se efectuó una revisión de cada uno de los controles y se los comparó con cada artículo de la LOPD con los que pueden tener concordancia.

A continuación, se presenta los resultados de este análisis de una manera resumida.

Tabla 6

Controles EGSI V2 con Artículos LOPD

No.	Descripción Control EGSI V2	Artículos LOPDP
1	Políticas de Seguridad de la Información	Artículos 37, 38, 10
2	Organización de la Seguridad de la Información	Arts. 10,11, 37, 39, 55,56,57,59,60
3	Seguridad de los recursos humanos	Arts. 12,13,14,15,16,17,18,19,26
4	Gestión de activos	Art. 40
5	Control de acceso	Arts. 34, 37, 38, 41
6	Criptografía	Arts. 37,38, 41
7	Seguridad física y del entorno	Arts. 37,38,41
8	Seguridad de las operaciones	Arts. 37,38,39,41,43,46
9	Seguridad en las comunicaciones	Arts. 55,56,57,59,60
10	Adquisición, desarrollo y mantenimiento de los sistemas	Art. 39
11	Relaciones con proveedores	Arts. 33, 55,56,57,59,60
12	Gestión de incidentes de seguridad de la información	Arts. 43,46
13	Aspectos de seguridad de la información para la gestión de la continuidad del negocio	Art. 61
14	Cumplimiento	Arts. 38,11

Nota. La tabla muestra los controles del EGSI que cumplen los artículos de la LOPDP.

Consideraciones para cumplimiento de Controles del EGSI basados en la LOPDP

En la tabla que se presenta a continuación se pude verificar las consideraciones que se debe tener en el INPC para cumplir con los artículos de la LOPDP.

Tabla 7

Consideraciones para cumplimiento de la LOPDP

Ítem		Descripción	Artículos de Cumple en la LOPD	Consideraciones Técnicas a Realizar para cumplimiento de LOPD	Costo USD
	1	**POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN**	**Arts. 37, 38, Principios**		
1.1.1.3		Las instituciones públicas podrán especificar y difundir una política de seguridad más amplia o específica en armonía con la Constitución, leyes y demás normativa legal propia o relacionada, así como su misión y competencias.		La política debe ser actualizada para incluir la protección de datos personales.	
	2	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**	**Principios, Arts. 11, 37, 38, 39, 41, 55,56,57,59,60**		
		La institución debe definir y asignar claramente todas las responsabilidades para la seguridad de la información		Generar la Política interna de Protección de Datos, designación de responsabilidades y normativa de la Ley y Reglamento.	
2.1.1.4		Definir y hacer cumplir lo definido para la coordinación y supervisión de seguridad de la información con los proveedores.		Crear procedimiento de tratamiento de información con proveedores.	
2.1.1.8		Asignar las responsabilidades para la seguridad de la información.		Asignar mediante memorando las responsabilidades para la seguridad de la información.	
2.1.2.1		Se debería cuidar el hecho de que una persona por sí sola no pueda acceder, modificar o utilizar los activos sin autorización o sin que se detecte.		Generar Política de Acceso a la Información incluido datos personales que no sean públicos.	

Ítem	Descripción	Artículos de Cumple en la LOPD	Consideraciones Técnicas a Realizar para cumplimiento de LOPD	Costo USD
2.1.4.3	Recibir avisos tempranos de alertas, asesoramiento y parches relacionados con ataques a las vulnerabilidades de la institución, por parte de instituciones públicas, privadas y académicas reconocidas por su aporte en la gestión de la seguridad de la información.		Generación de procedimiento de consulta de vulnerabilidades en la Unidad de TI.	
2.1.4.4	Obtener acceso a asesoramiento especializado en seguridad de la información con instituciones públicas o privadas especializadas en seguridad de la información.		Generar reuniones con la Dirección Nacional de Registro de Datos Públicos y Mintel para apoyarse en la implementación de normativa.	
2.1.5.1	Los objetivos de seguridad de la información estén incluidos en los objetivos del proyecto, de ser pertinente.		Aumentar en específico el tratamiento de datos personales.	
2.1.5.2	Determinar los riesgos de seguridad de la información para identificar e implementar los controles necesarios.		Aumentar riesgos de seguridad de la información haciendo énfasis sobre protección de datos personales.	
2.1.6.1	Identificar requisitos de seguridad antes de facilitar servicios a ciudadanos o clientes de instituciones gubernamentales. que utilicen o procesen información de los mismos o de la institución. Se podrá utilizar los siguientes criterios:		Generar proceso de tratamiento de datos personales en servicios que brinda la institución tanto virtuales como presenciales.	
2.1.6.1.1	Protección de activos de información.		Añadir a los datos personales como un activo e información.	

Ítem	Descripción	Artículos de Cumple en la LOPD	Consideraciones Técnicas a Realizar para cumplimiento de LOPD	Costo USD
2.1.6.1.4	Política de control del acceso.		Aumentar en la política el acceso a datos personales.	
2.1.6.1.5	Convenios para gestión de inexactitudes de la información, incidentes de la Seguridad de la información y violaciones de la seguridad.		Establecer la Política de Tratamiento de Datos Personales en la que se debe incluir la gestión del proceso administrativo.	
2.1.6.1.9	Las respectivas responsabilidades civiles de la institución y del cliente		Actualizar políticas de privacidad en sistemas de información de servicios en línea.	
2.1.6.1.12	Protección de datos en base la Constitución y leyes nacionales, particularmente datos personales o financieros de los ciudadanos.		Política, procesos y procedimientos internos de protección de datos personales.	
2.2.2.18	Definir los procedimientos para las copias de respaldo y para la continuidad del negocio.		Generar Política de Respaldos de Información, Adquisición de software para respaldos automáticos en librería de cintas	11000
2.2.2.19	Establecer los requisitos necesarios para la auditoría y monitoreo de seguridad.		Conexión mediante VPN para registrar los accesos a los sistemas y tiempo de conexión.	
3	**Seguridad de los recursos humanos.**	**Arts. 7,8,9,12,13,14,15,16,17,18,19,26**		

Ítem	Descripción	Artículos de Cumple en la LOPD	Consideraciones Técnicas a Realizar para cumplimiento de LOPD	Costo USD
	Verificar antecedentes de candidatos a ser empleados, contratistas o usuarios de terceras partes, designaciones y promociones de funcionarios de acuerdo con los reglamentos, la ética y las leyes pertinentes, y deben ser proporcionales a la naturaleza y actividades de la institución pública, a la clasificación de la información a la cual se va a tener acceso y los riesgos percibidos. No debe entenderse este control como discriminatorio en ningún aspecto.		Procedimiento de la Dirección de Administración del TTHH que indique el tratamiento de la información recabada en hojas de vida y documentación requerida.	
	Los funcionarios, contratistas y terceros deben aceptar y firmar los términos y condiciones del contrato de trabajo, el cual establece sus responsabilidades y obligaciones de acuerdo a la norma legal vigente.		Actualización de contratos debe estar incluido en el procedimiento de la Dirección de Administración del TTHH.	

Ítem	Descripción	Artículos de Cumple en la LOPD	Consideraciones Técnicas a Realizar para cumplimiento de LOPD	Costo USD
3.1.2.1	Realizar la firma del acuerdo de confidencialidad o no-divulgación, antes de que los empleados, contratistas y usuarios de terceras partes, tengan acceso a la información. Dicho acuerdo debe establecer los parámetros tanto de vigencia del acuerdo, información confidencial referida, formas de acceso, responsabilidades y funciones.;		Procedimiento de la Dirección de Administración del TTHH que indique el tratamiento de la información recabada en hojas de vida y documentación requerida.	
	Exigir a los funcionarios, contratistas que se aplique la seguridad de la información, de acuerdo con las políticas y procedimientos definidos por la institución		Seguridad de la Información y Responsable de Tratamiento de Datos institucional, mediante normativa interna.	
3.2.1.4	Acordar los términos y las condiciones laborales, las cuales incluyen la política de la seguridad de la información de la institución y los métodos apropiados de trabajo;		Procedimiento de la Dirección de Administración del TTHH que indique el tratamiento de la información recabada en hojas de vida y documentación requerida.	
4	**Gestión de activos**	**Arts. 25,26,40,41**		
	Inventariar, identificar y actualizar todos los activos asociados con la información, y las instalaciones para el procesamiento de la información.		Se puede basar en directrices de Mintel, matrices entregadas, incluyendo a los datos personales como un activo más.	
4.1.1.2	Inventariar los activos de soporte de Hardware.		Implementación de software de inventarios (OCS Inventory) capacidad instalada.	

Ítem	Descripción	Artículos de Cumple en la LOPD	Consideraciones Técnicas a Realizar para cumplimiento de LOPD	Costo USD
4.1.2.4	Asegurar el manejo adecuado para el borrado o destrucción del activo.		Borrado de información con herramientas basadas en software libre.	
4.1.3.1	Para la elaboración de las reglas, el responsable del Activo deberá tomar en cuenta las actividades definidas en los controles correspondientes a los ámbitos de "Intercambio de Información" y "Control de Acceso", donde sea aplicable.		Política interna de Tratamiento de Personales, procedimiento de intercambio de información según artículos de la LOPDP.	
4.1.3.4.3	Todos los mensajes deben poder ser monitoreados y conservados permanentemente por parte de las instituciones.		Generar Política de Respaldos de Información, adquisición de software para respaldos automáticos en librería de cintas.	
4.1.3.4.8	Deben utilizarse programas que monitoreen el accionar de virus informáticos tanto en mensajes como en archivos adjuntos, antes de su ejecución.		Adquisición de Soluciones de Antivirus y anti spam.	3000

Ítem	Descripción	Artículos de Cumple en la LOPD	Consideraciones Técnicas a Realizar para cumplimiento de LOPD	Costo USD
4.1.3.5.3	Debe limitarse a los usuarios el acceso a portales, aplicaciones o servicios de la Internet y la Web que pudieren perjudicar los intereses y la reputación de la institución. Específicamente, se debe bloquear el acceso por medio de dispositivos fijos y/o móviles a aquellos portales, aplicaciones o servicios de la Internet y la Web sobre pornografía, racismo, violencia, delincuencia o de contenidos ofensivos y contrarios a los intereses, entre otros, y valores de la institución o que impacten negativamente en la productividad y trabajo de la institución (ej., mensajería instantánea-chats, redes sociales, video, otros) y particularmente a los que atenten a la ética y moral.		Compra de equipo de seguridad perimetral (Firewall) de próxima Generación.	6800
4.2.2.3	En caso de documentos en formato electrónico, la etiqueta deberá asociarse a un metadato único, pudiendo ser éste un código MD5.		Implementación de herramientas para cifrado de información libres o gratuitas como QuickHash, MultiHasher	

Ítem	Descripción	Artículos de Cumple en la LOPD	Consideraciones Técnicas a Realizar para cumplimiento de LOPD	Costo USD
	Implementar procedimientos para la gestión de los medios extraíbles, de acuerdo con el esquema de clasificación implementado por la institución, se debe documentar los procedimientos y los niveles de autorización.		El procedimiento de gestión de medios extraíbles, debe definir medios que contengan datos personales y/o datos públicos y su respectivo tratamiento.	
5	**Control de acceso**	**Arts. 34, 37, 38, 41**	**Implementación de sistemas de control de accesos, con tarjetas magnéticas para un mejor control**	5500
5.2.1.9	Mantener un registro de la gestión de accesos a aplicaciones, redes, que evidencie, fecha de creación, eliminación, suspensión, activación o eliminación del acceso; al igual que de cada usuario, disponer de los permisos de acceso que han sido asignados.		Implementación de módulos de auditoria en los sistemas de información institucionales, (capacidad instalada).	
5.4.1.3	Implementar controles sobre los perfiles de acceso de los usuarios, por ejemplo, de lectura, de escritura, de borrado y de ejecución de la información. etc.;		Modificación/Actualización de Sistemas de Información ya que se encuentran desarrollados en software que ya tienen varios años de uso, y la tecnología debe ser actualizada, además de implementar un diseño de roles y perfiles. (capacidad instalada).	

Ítem	Descripción	Artículos de Cumple en la LOPD	Consideraciones Técnicas a Realizar para cumplimiento de LOPD	Costo USD
5.4.4.1.1	Utilizar un manejador de versiones para el código fuente, proporcionar permisos de acceso a los desarrolladores bajo autorizaciones.		Implementar software libre u open source como GIT, Apache Subversion (capacidad instalada).	
6	**Criptografía**	**Arts. 37,38, 41**		
	Elaborar, implementar y socializar una política que regule el uso de controles criptográficos para la protección de la información, de acuerdo al nivel de protección requerida.		Implementación de uso de herramientas cryptográficas en software libre como Cryptomator u otra similar (capacidad instalada).	
7	**Seguridad física y del entorno**	**Arts. 37,38,41**		
7.2.1.10	Proteger los equipos que procesan la información sensible para minimizar el riesgo de fugas de información debidas a una emanación electromagnética.		Hardenización de Servidores (capacidad instalada).	
	Los equipos deberían estar protegidos contra cortes de luz y otras interrupciones provocadas por fallas en los suministros básicos de apoyo.		Compra de UPS para equipos, ya que el edificio no cuenta con energía de respaldo en todas las estaciones de trabajo (100).	8000
	Los cables eléctricos y de telecomunicaciones que transportan datos o apoyan a los servicios de información se deberían proteger contra la intercepción, interferencia o posibles daños.		Renovación de cableado estructurado.	no definido
8	**Seguridad de las operaciones**	**Arts.37,38,39,41,43,46**		

Ítem	Descripción	Artículos de Cumple en la LOPD	Consideraciones Técnicas a Realizar para cumplimiento de LOPD	Costo USD
8.1.4	Separación de ambientes de desarrollo, pruebas y producción.		Habilitación del 2do centro de datos.	5800
8.4.4	Sincronización de relojes.		Implementación de servidor NTP (capacidad instalada).	
9	**Seguridad en las comunicaciones**	**Arts. 55,56,57,59,60**		
9.1.2.1	Incorporar tecnología aplicada para la seguridad de los servicios de red, como la autenticación, cifrada y controles de conexión de red.		Actualización/cambio de Controlador de Wi-FI, actualmente se lo realiza solo por software.	no definido
	Elaborar implementar políticas, procedimientos y controles formales que protejan la transferencia de información que viaja a través del uso de todo tipo de recursos de comunicación.		Implementación de software WireShark o similares (capacidad instalada).	
10	**Adquisición, desarrollo y mantenimiento de los sistemas**	**Art. 39**		
10.1.1.1	Definir los requerimientos de seguridad. Por ejemplo: criptografía, control de sesiones, etc.		Actualización de sistemas o desarrollo de sistemas con manejo de seguridad de la información (capacidad instalada).	
11	**Relaciones con proveedores**	**Arts. 33, 55,56,57,59,60**		
12	**Gestión de incidentes de seguridad de la información**	**Arts. 43,46**		
13	**Aspectos de seguridad de la información para la gestión de la continuidad del negocio**	**Art. 61**		

Ítem	Descripción	Artículos de Cumple en la LOPD	Consideraciones Técnicas a Realizar para cumplimiento de LOPD	Costo USD
	La institución debe determinar sus necesidades de seguridad de la información y la continuidad de su gestión de seguridad de la información, en situaciones adversas como una crisis o un desastre.		Implementación de un centro de datos alterno virtual.	No definido
14	**Cumplimiento**	**Arts. 38,11**		

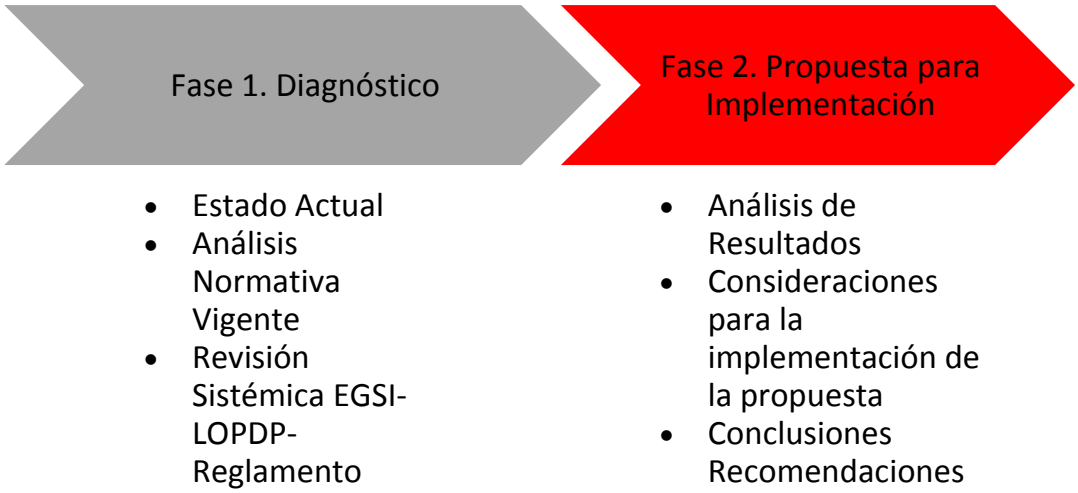
Nota. La tabla muestra las consideraciones que se debe tomar en cuenta para cumplir con la normativa de LOPDP y EGSI.

Los costos que se encuentran descritos en la tabla fueron tomados de cotizaciones reales de procesos de compras públicas que realizó la institución en el transcurso del año en curso para la adquisición de equipamiento informático.

a. Estructura general

Figura 11

Estructura General de la Propuesta



Nota. La figura indica las fases que contiene la estructura general del trabajo de investigación.

b. Explicación del aporte

El trabajo de investigación contribuirá directamente al INPC para la implementación de la normativa emitida desde los entes rectores, lo que promoverá el aumento de la seguridad de la información en el tratamiento de datos personales en los sistemas que actualmente son considerados servicios públicos y que están al servicio de la ciudadanía en general, como son: Autorización de Movilización de Bienes Culturales, Registro de Profesionales, Servicios Especializados de Laboratorio, Sistema de Información del Patrimonio Cultural, entre otros, todos estos recopilan información y datos personales.

El documento también proporcionará información útil, como las consideraciones y ciertos procedimientos para implementar un esquema de seguridad de la información y tratamiento de datos personales a nivel gubernamental con base en la normativa ecuatoriana, lo que favorece al aumento de confianza en el manejo de información en sistemas de información a nivel de Gobierno Electrónico.

c. Estrategias y/o técnicas

Búsqueda bibliográfica

Es una técnica de investigación documental que sirve para cualquier clase de estudio. Consiste en buscar fuentes de información afines al trabajo de investigación a desarrollar, estas pueden ser de diferentes tipos, como libros, revistas, tesis, artículos científicos, entre otros.

Se constituye como el primer paso y base de toda investigación, puesto que se aproxima al conocimiento de un tema para identificar qué se sabe y qué se desconoce. Los investigadores pueden realizar con mejor precisión el estudio, contribuye a mejorar la interpretación de ideas y resultados mediante la discusión de los diferentes autores, y garantiza la obtención de información más relevante en el tema a desarrollarse.

Además, que es fundamental en los procesos de meta-análisis, meta-síntesis y revisión sistemática porque ayuda a identificar, seleccionar, sintetizar y valorar las diferentes investigaciones con el fin de desarrollar una mejor visión de un tema.

Encuesta

La encuesta es una interrogación verbal o escrita que se efectúa a personas para obtener determinada información que es fundamental para una investigación. Esta técnica es de múltiple aplicación y gran alcance, lo que le convierte en un instrumento de gran utilidad en cualquier tipo de estudio, además que es ampliamente utilizada porque permite obtener y elaborar datos de modo rápido y eficaz.

Mediante esta se recoge y analiza información y ciertos datos de una muestra o población representativa, de la que se pretende obtener, explorar, describir y explicar una serie de características.

Para el desarrollo del presente trabajo se ha considerado principalmente estas dos técnicas de investigación. En el caso de la búsqueda bibliográfica porque como se menciona anteriormente, es el primer paso y base de toda investigación. Es importante contar con varios contextos y aportaciones de otras fuentes y estudios realizados, para generar opiniones y propuestas sustentadas. Y las entrevistas puesto que, mediante el cuestionario se puede obtener información precisa y lograr un mayor acopio de la información en torno a la temática planteada.

1.3. Validación de la propuesta

No se puede realizar una validación ya que este documento es solamente una propuesta de varias consideraciones que se debe tener en cuenta para la implementación de un esquema de seguridad de la información con enfoque en la protección de datos personales.

Se pondrá en conocimiento de las partes interesadas, al director de Planificación y Gestión Estratégica y la Dirección Ejecutiva del INPC para que se analice su posible implementación.

CONCLUSIONES

Una vez que se ha concluido con el presente trabajo de investigación se ha llegado a las siguientes conclusiones:

1. Ecuador carece de la emisión de un Reglamento a la Ley Orgánica de Protección de Datos Personales por lo que es necesario basarse en el reglamento de un país de la región latinoamericana como es Perú.
2. Al analizar el Reglamento de la Ley N^{o} 29733 - Ley de Protección de Datos Personales de Perú, se puede evidenciar que, el tratamiento de datos personales y la normativa propuesta en la LOPDP de Ecuador existente una similitud del 93% ya que en los artículos revisados solamente dos no tienen una correspondencia directa.
3. Con los resultados de la encuesta realizada se pone en evidencia que en el Instituto Nacional de Patrimonio Cultural los funcionarios alcanzan un 69,35% de conocimiento sobre la existencia de la normativa tanto de Seguridad de la Información, EGSI y Ley Orgánica de Protección de Datos Personales.
4. Una vez terminado el estudio se verifica que las normativas de protección de datos personales y de seguridad de la información son complementarias y que pueden ser implementadas orientando ciertos controles hacia la protección de datos personales, sin necesidad de crear un procedimiento exclusivo para este tema. Los artículos que se verificaron que son de obligatorio cumplimiento en la institución pueden ser cumplidos al 100% generando las políticas, procesos y procedimientos necesarios, así como realizando una inversión aproximada de USD. $ 40.100,00 (Cuarenta mil cien con 00/100 dólares de los estados Unidos de Norteamérica) en equipamiento tecnológico y software requerido.
5. La mayoría de los controles y artículos de la normativa tanto del EGSI y de la LOPDP se cumplen con la aplicación de políticas, procesos y procedimientos que pueden ser generados internamente en la institución con capacidad instalada y sin la necesidad de generar gastos extras.
6. Aplicando las consideraciones expuestas en este documento, al conocer que el INPC maneja información de personas naturales y jurídicas que tienen en su poder patrimonios culturales invaluables, la implementación del EGSI basado en la protección de datos personales, es de vital ayuda en la conservación y mitigación de robo de información que pueda atentar contra los patrimonios culturales del Ecuador.

RECOMENDACIONES

1. Al no contar con un Reglamento a la LOPD es primordial revisar los diferentes reglamentos y leyes de otros países, así no se exime de responsabilidades y se da cumplimiento adecuadamente a la ley con apoyo en estándares y prácticas internacionales.
2. Al concluir que los funcionarios del INPC tienen conocimientos básicos de las normativas, se recomienda socializar y concientizar sobre la importancia de estas, para salvaguardar la información y disminuir situaciones que comprometan la seguridad de la información.
3. El presente documento ofrece una oportunidad para que futuras investigaciones realicen más estudios sobre la seguridad de la información y su implementación en las diferentes instituciones con base en la normativa existente, pero es importante que consideren el tipo de organización ya que no todas tienen las mismas necesidades de seguridad, sus riesgos pueden variar de acuerdo con su naturaleza y procesos.
4. Evaluar y aprobar las consideraciones mencionadas en el presente trabajo de investigación para aplicar en la institución. Así como, implementar el EGSI con énfasis en la protección de datos a fin de normar toda actividad relacionada a la seguridad de la información.
5. Trabajar en conjunto y apoyar al área de sistemas en temas relacionados con la seguridad de la información para garantizar la confidencialidad, integridad y disponibilidad de esta en los diferentes procesos que se llevan a cabo la institución.

BIBLIOGRAFÍA

Borja Morales, J. X. (2019). *La inadecuada regulación para la protección de datos personales en el ordenamiento jurídico del Ecuador*. http://dspace.udla.edu.ec/handle/33000/11102

Corletti Estrada, A. (2017). Ciberseguridad: Una estrategia Informático Militar. *Madrid: DarFe*.

De la Mata, J. Z., & Lería, I. M. A. (2008). *Protección de datos: Comentarios al reglamento*. Lex Nova.

EGSI v2. (s. f.). *Gobierno Electrónico de Ecuador*. Recuperado 27 de abril de 2022, de https://www.gobiernoelectronico.gob.ec/egsi-v2/

Enríquez Álvarez, L. F. (2017). *Paradigmas de la protección de datos personales en Ecuador. Análisis del proyecto de Ley Orgánica de Protección a los Derechos a la Intimidad y Privacidad sobre los Datos Personales (Tema Central)*. http://repositorio.uasb.edu.ec/handle/10644/5945

Figueroa-Suárez, J. A., Rodríguez-Andrade, R. F., Bone-Obando, C. C., & Saltos-Gómez, J. A. (2018). La seguridad informática y la seguridad de la información. *Polo del Conocimiento*, *2*(12), 145.

Gascó, G. E. (2013). *Seguridad informática*. Macmillan Iberia, S.A. https://elibro.net/es/ereader/uisrael/43260

Gobierno de Perú (22 marzo, 2013) Reglamento de la Ley No 29733, Ley de Protección de Datos Asamblea Nacional (mayo 26, 2021). Ley Orgánica de Protección de Datos Personales.

Ministerio de Cultura y Patrimonio (febrero 07, 2019). Acuerdo Ministerial Nro DM-2019-019.

Ministerio de Telecomunicaciones y de la Sociedad de la Información (agosto 18, 2019). Acuerdo Ministerial 12

REGLAMENTO (UE) 2016/ 679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO - de 27 de abril de 2016—

Relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/ 46/ CE (Reglamento general de protección de datos). (s. f.). 88.

Roldán Carrillo, F. N. (2020). *Los ejes centrales de la protección de datos: Consentimiento y finalidad. Críticas y propuestas hacia una regulación de la protección de datos personales en Ecuador*. http://repositorio.usfq.edu.ec/handle/23000/9952

Tenorio Pereyra, J. E. (2018). *Desafíos y oportunidades de la adhesión del Perú al Convenio de Budapest sobre la Ciberdelincuencia*.

Torres, R. H. S. (2019). *Metodología de la investigación. Las rutas cuantitativa, cualitativa y mixta*. México: Mc Graw Hill Interamericana Editores, SA de CV.

Transparencia – Instituto Nacional de Patrimonio Cultural. (s. f.). Recuperado 27 de abril de 2022, de https://www.patrimoniocultural.gob.ec/transparencia/

ANEXOS

ANEXO 1: Formato De Encuesta

ENCUESTA CONOCIMIENTO SEGURIDAD DE LA INFORMACIÓN

La presente encuesta tiene como objeto saber el nivel de conocimiento de los funcionarios sobre la seguridad de la información y la Ley Orgánica de Protección de Datos Personales

¿Sabe qué es la Seguridad de la Información?

Si

No

Seleccione un concepto que defina la seguridad de la información

Conjunto de medidas preventivas y reactivas que permiten resguardar y proteger la información

Conjunto de medidas para el bloqueo de acceso a internet

¿Tiene conocimiento sobre el Esquema Gubernamental de Seguridad de la Información (EGSI)?

SI

NO

¿Conoce si en la institución se aplica el EGSI?

SI

NO

¿Tiene conocimiento que en el país desde el año 2021 existe una Ley Orgánica de Protección de Datos Personales?

SI

NO

Marque las opciones que considere son datos sensibles

Número de teléfono

Etnia

Orientación Sexual

¿Conoce sus derechos como titular de datos personales?

SI

NO

¿Sabe usted que puede oponerse o negarse al tratamiento de sus datos personales cuando se tenga por objeto la mercadotecnia?

SI

NO

ANEXO 2: Revisión Sistémica LOPDP – Reglamento (Perú)

LOPDP	Reglamento de la ley No 29733, Ley de Protección de Datos Personales
Art. 7.- Tratamiento legítimo de datos personales. - El tratamiento será legítimo y lícito si se cumple con alguna de las siguientes condiciones: 1) Por consentimiento del titular para el tratamiento de sus datos personales, para una o varias finalidades especificas; 2) Que sea realizado por el responsable del tratamiento en cumplimiento de una obligación legal; 3) Que sea realizado por el responsable del tratamiento, per orden judicial, debiendo observarse los principios de la presente ley; 4) Que el tratamiento de datos personales se sustente en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, derivados de una competencia atribuida por una norma con rango de ley, sujeto al cumplimiento de los estándares internacionales de derechos humanos aplicables a la materia, al cumplimiento de los principios de esta ley y a los criterios de legalidad, proporcionalidad y necesidad; 5) Para la ejecución de medidas precontractuales a petición del titular o para el cumplimiento de obligaciones contractuales perseguidas por el responsable del tratamiento de datos personales, encargado del tratamiento de datos personales o por un tercero legalmente habilitado; 6) Para proteger intereses vitales, del interesado o de otra persona natural, como su vida, salud o integridad, 7) Para tratamiento de datos personales que consten en bases de datos de acceso público; u, 8) Para satisfacer un interés legítimo del responsable de tratamiento o de tercero, siempre que no prevalezca el interés o derechos fundamentales de los titulares al amparo de lo dispuesto en esta norma.	**Tratamiento de datos personales** **Capítulo I** **Consentimiento** **Artículo 11.- Disposiciones generales sobre el consentimiento para el tratamiento de datos personales.** El titular del banco de datos personales o quien resulte como responsable del tratamiento, deberá obtener el consentimiento para el tratamiento de los datos personales, de conformidad con lo establecido en la Ley y en el presente reglamento, salvo los supuestos establecidos en el artículo 14 de la Ley, en cuyo numeral 1) queda comprendido el tratamiento de datos personales que resulte imprescindible para ejecutar la interoperabilidad entre las entidades públicas. La solicitud del consentimiento deberá estar referida a un tratamiento o serie de tratamientos determinados, con expresa identificación de la finalidad o finalidades para las que se recaban los datos; así como las demás condiciones que concurran en el tratamiento o tratamientos, sin perjuicio de lo dispuesto en el artículo siguiente sobre las características del consentimiento. Cuando se solicite el consentimiento para una forma de tratamiento que incluya o pueda incluir la transferencia nacional o internacional de los datos, el titular de los mismos deberá ser informado de forma que conozca inequívocamente tal circunstancia, además de la finalidad a la que se destinarán sus datos y el tipo de actividad desarrollada por quien recibirá los mismos. **Artículo 12.- Características del consentimiento.** Además de lo dispuesto en el artículo 18 de la Ley y en el artículo precedente del presente reglamento, la obtención del consentimiento debe ser: **1. Libre**: Sin que medie error, mala fe, violencia o dolo que puedan afectar la manifestación de voluntad del titular de los datos personales. La entrega de obsequios o el otorgamiento de beneficios al titular de los datos personales con ocasión de su consentimiento no afectan la condición de libertad que tiene para otorgarlo, salvo en el caso de menores de edad, en los supuestos en que se

admite su consentimiento, en que no se considerará libre el consentimiento otorgado mediando obsequios o beneficios.

El condicionamiento de la prestación de un servicio, o la advertencia o amenaza de denegar el acceso a beneficios o servicios que normalmente son de acceso no restringido, sí afecta la libertad de quien otorga consentimiento para el tratamiento de sus datos personales, si los datos solicitados no son indispensables para la prestación de los beneficios o servicios.

2. Previo: Con anterioridad a la recopilación de los datos o en su caso, anterior al tratamiento distinto a aquel por el cual ya se recopilaron.

3. Expreso e Inequívoco: Cuando el consentimiento haya sido manifestado en condiciones que no admitan dudas de su otorgamiento.

Se considera que el consentimiento expreso se otorgó verbalmente cuando el titular lo exterioriza oralmente de manera presencial o mediante el uso de cualquier tecnología que permita la interlocución oral.

Se considera consentimiento escrito a aquél que otorga el titular mediante un documento con su firma autógrafa, huella dactilar o cualquier otro mecanismo autorizado por el ordenamiento jurídico que queda o pueda ser impreso en una superficie de papel o similar.

La condición de expreso no se limita a la manifestación verbal o escrita.

En sentido restrictivo y siempre de acuerdo con lo dispuesto por el artículo 7 del presente reglamento, se considerará consentimiento expreso a aquel que se manifieste mediante la conducta del titular que evidencie que ha consentido inequívocamente, dado que de lo contrario su conducta, necesariamente, hubiera sido otra.

Tratándose del entorno digital, también se considera expresa la manifestación consistente en “hacer clic”, “cliquear” o “pinchar”, “dar un toque”, “touch” o “pad” u otros similares.

En este contexto el consentimiento escrito podrá otorgarse mediante firma electrónica, mediante escritura que quede grabada, de forma tal que pueda ser leída e impresa, o que por cualquier otro mecanismo o procedimiento establecido permita identificar al titular y recabar su consentimiento, a través de texto escrito. También podrá otorgarse mediante texto preestablecido, fácilmente visible, legible y en lenguaje sencillo, que el titular pueda hacer suyo, o no, mediante una respuesta escrita, gráfica o mediante clic o pinchado.

La sola conducta de expresar voluntad en cualquiera de las formas reguladas en el presente numeral no elimina, ni da por cumplidos, los otros requisitos del consentimiento referidos a la libertad, oportunidad e información.

4. Informado: Cuando al titular de los datos personales se le comunique clara, expresa e indubitablemente, con lenguaje sencillo, cuando menos de lo siguiente:

a. La identidad y domicilio o dirección del titular del banco de datos personales o del responsable del tratamiento al que puede dirigirse para revocar el consentimiento o ejercer sus derechos.

b. La finalidad o finalidades del tratamiento a las que sus datos serán sometidos.

c. La identidad de los que son o pueden ser sus destinatarios, de ser el caso.

d. La existencia del banco de datos personales en que se almacenarán, cuando corresponda.

e. El carácter obligatorio o facultativo de sus respuestas al cuestionario que se le proponga, cuando sea el caso.

f. Las consecuencias de proporcionar sus datos personales y de su negativa a hacerlo.

g. En su caso, la transferencia nacional e internacional de datos que se efectúen.

Artículo 13.- Políticas de privacidad.

La publicación de políticas de privacidad, de acuerdo a lo previsto en el segundo párrafo del artículo 18 de la Ley, debe entenderse como una forma de cumplimiento del deber de información que no exonera del requisito de obtener el consentimiento del titular de los datos personales.

Artículo 14.- Consentimiento y datos sensibles.

Tratándose de datos sensibles, el consentimiento debe ser otorgado por escrito, a través de su firma manuscrita, firma digital o cualquier otro mecanismo de autenticación que garantice la voluntad inequívoca del titular.

Artículo 15.- Consentimiento y carga de la prueba.

Para efectos de demostrar la obtención del consentimiento en los términos establecidos en la Ley y en el presente reglamento, la carga de la prueba recaerá en todos los casos en el titular del banco de datos personales o quien resulte el responsable del tratamiento.

Artículo 16.- Negación, revocación y alcances del consentimiento.

LOPDP	Reglamento de la ley No 29733, Ley de Protección de Datos Personales
	El titular de los datos personales podrá revocar su consentimiento para el tratamiento de sus datos personales en cualquier momento, sin justificación previa y sin que le atribuyan efectos retroactivos. Para la revocación del consentimiento se cumplirán los mismos requisitos observados con ocasión de su otorgamiento, pudiendo ser estos más simples, si así se hubiera señalado en tal oportunidad. El titular de los datos personales podrá negar o revocar su consentimiento al tratamiento de sus datos personales para finalidades adicionales a aquellas que dan lugar a su tratamiento autorizado, sin que ello afecte la relación que da lugar al consentimiento que sí ha otorgado o no ha revocado. En caso de revocatoria, es obligación de quien efectúa el tratamiento de los datos personales adecuar los nuevos tratamientos a la revocatoria y los tratamientos que estuvieran en proceso de efectuarse, en el plazo que resulte de una actuación diligente, que no podrá ser mayor a cinco (5) días. Si la revocatoria afecta la totalidad del tratamiento de datos personales que se venía haciendo, el titular o encargado del banco de datos personales, o en su caso el responsable del tratamiento, aplicará las reglas de cancelación o supresión de datos personales. El titular del banco de datos personales o quien resulte responsable del tratamiento debe establecer mecanismos fácilmente accesibles e incondicionales, sencillos, rápidos y gratuitos para hacer efectiva la revocación.
Art. 8.- Consentimiento. - Se podrán tratar y comunicar datos personales cuando se cuentan con la manifestación del titular para hacerlo. El consentimiento será válido, cuando la manifestación de la voluntad sea: 1) Libre, es decir, cuando se encuentre exenta de vicios del consentimiento; 2) Específica, en cuanto a la determinación concreta de los medios y fines del tratamiento; 3) Informada, de modo que cumpla con el principio de transparencia y efectivice el derecho a la transparencia, 4) Inequívoca, de manera que no presente dudas sobre el alcance de la autorización otorgada por el titular. El consentimiento podrá revocarse en cualquier momento sin que sea necesaria una justificación., para lo cual el responsable del tratamiento de datos personales establecerá mecanismos que garanticen celeridad,	**Los articulo anteriormente descritos** **Tratamiento de datos personales** **Capítulo I** **Consentimiento** **Artículos 11, 12, 13, 14, 15, 16.** **Capítulo II** **Limitaciones al consentimiento** **Artículo 17.- Fuentes accesibles al público**. Para los efectos del artículo 2, inciso 9) de la Ley, se considerarán fuentes accesibles al público, con independencia de que el acceso requiera contraprestación, las siguientes: 1. Los medios de comunicación electrónica, óptica y de otra tecnología, siempre que el lugar en el que se encuentren los datos personales esté concebido para facilitar información al público y esté abierto a la consulta general.

LOPDP	Reglamento de la ley No 29733, Ley de Protección de Datos Personales
eficiencia, eficacia y gratuidad, así como un procedimiento sencillo, similar al proceder con el cual recabó el consentimiento. El tratamiento realizado antes de revocar el consentimiento es lícito, en virtud de que este no tiene efectos retroactivos. Cuando se pretenda fundar el tratamiento de los datos en el consentimiento del afectado Dará una pluralidad de finalidades será preciso que conste que dicho consentimiento se otorga para todas ellas.	2. Las guías telefónicas, independientemente del soporte en el que estén a disposición y en los términos de su regulación específica. 3. Los diarios y revistas independientemente del soporte en el que estén a disposición y en los términos de su regulación específica. 4. Los medios de comunicación social. 5. Las listas de personas pertenecientes a grupos profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección postal, número telefónico, número de fax, dirección de correo electrónico y aquellos que establezcan su pertenencia al grupo. En el caso de colegios profesionales, podrán indicarse además los siguientes datos de sus miembros: número de colegiatura, fecha de incorporación y situación gremial en relación al ejercicio profesional. 6. Los repertorios de jurisprudencia, debidamente anonimizados. 7. Los Registros Públicos administrados por la Superintendencia Nacional de Registros Públicos SUNARP, así como todo otro registro o banco de datos calificado como público conforme a ley.8. Las entidades de la Administración Pública, en relación a la información que deba ser entregada en aplicación de la Ley Nº 27806, Ley de Transparencia y Acceso a la Información Pública. Lo dispuesto en el numeral precedente no quiere decir que todo dato personal contenido en información administrada por las entidades sujetas a la Ley de Transparencia y Acceso a la Información Pública sea considerado información pública accesible. La evaluación del acceso a datos personales en posesión de entidades de administración pública se hará atendiendo a las circunstancias de cada caso concreto. El tratamiento de los datos personales obtenidos a través de fuentes de acceso público deberá respetar los principios establecidos en la Ley y en el presente reglamento
Art. 9.- Interés legítimo. – Cuando el tratamiento de datos personales tiene como fundamente el interés legítimo: a) Únicamente podrán ser tratados los datos que sean estrictamente necesarios para la realización de la finalidad. b) El responsable debe garantizar que el tratamiento sea transparente para el titular. c) La Autoridad de Protección de Datos puede requerir al responsable un informe con de riesgo para la protección de daros, en el cual se verificará si no	**Artículo 8.- Principio de finalidad.** En atención al principio de finalidad se considera que una finalidad está determinada cuando haya sido expresada con claridad, sin lugar a confusión y cuando de manera objetiva se especifica el objeto que tendrá el tratamiento de los datos personales. Tratándose de banco de datos personales que contengan datos sensibles, su creación solo puede justificarse si su finalidad además de ser legítima, es concreta y acorde con las actividades o fines explícitos del titular del banco de datos personales. Los profesionales que realicen el tratamiento de algún dato personal, además de estar

LOPDP	Reglamento de la ley No 29733, Ley de Protección de Datos Personales
hay amenazas concretas a las expectativas legitimas de los titúlales y a sus derechos fundamentales. **Art. 10.- Principios. -** Sin perjuicio de otros principios establecidos en la Constitución de la República, los instrumentos internacionales ratificados por el Estado u otras normas jurídicas, la presente Ley se regirá por los principios de; **a) Juridicidad. -** Los datos personales deben tratarse con estricto apego y cumplimiento a los principios, derechos y obligaciones establecidas en la Constitución, los instrumentos internacionales, la presente Ley, su Reglamento y la demás normativa y jurisprudencia aplicable. **b) Lealtad**. – El tratamiento de datos personales deberá ser leal, por lo que para los titulares debe quedar claro que se están recogiendo, utilizando, consultando o tratando de otra manera, datos personales que les conciernen, así como las formas en que dichos datos son o serán tratados. En ningún caso los datos personales podrán ser tratados a través de medios o para fines, ilícitos o desleales. **c) Transparencia. -** El tratamiento de cacos personales deberá ser transparente. Por lo que toda información o comunicación relativa a este tratamiento deberá ser fácilmente accesible y fácil de entender y se deberá utilizar un lenguaje sencillo y claro. Las relaciones derivadas del tratamiento de datos personales deben ser transparentes y se rigen en función de las disposiciones contenidas en la presente Ley, su reglamento y demás normativa atinente a la materia. **d) Finalidad. -** Las finalidades del tratamiento deberán ser determinadas, explícitas, legítimas y comunicadas al titular; no podrán tratarse datos personales con fines distintos para los cuales fueron recopilados, a menos que concurra una de las causales que habiliten un nuevo tratamiento conforme los supuestos de tratamiento legítimo señalados en esta ley. El tratamiento de datos personales con fines distintos de aquellos para los que hayan sido recogidos inicialmente solo debe permitirse cuando sea compatible con los fines de su recogida inicial. Para ello, habrá de considerarse el contexto en el que se recogieron los datos, la información facilitada al titular en ese proceso y, en particular, las expectativas razonables del titular basadas	limitados por la finalidad de sus servicios, se encuentran obligados a guardar secreto profesional. **TÍTULO II** **Principios rectores** **Artículo 6.- Principios rectores**. El titular del banco de datos personales, o en su caso, quien resulte responsable del tratamiento, debe cumplir con los principios rectores de la protección de datos personales, de conformidad con lo establecido en la Ley, aplicando los criterios de desarrollo que se establecen en el presente título del reglamento. **Artículo 7.- Principio de consentimiento.** En atención al principio de consentimiento, el tratamiento de los datos personales es lícito cuando el titular del dato personal hubiere prestado su consentimiento libre, previo, expreso, informado e inequívoco. No se admiten fórmulas de consentimiento en las que éste no sea expresado de forma directa, como aquellas en las que se requiere presumir, o asumir la existencia de una voluntad que no ha sido expresa. Incluso el consentimiento prestado con otras declaraciones, deberá manifestarse en forma expresa y clara. **Artículo 8.- Principio de finalidad.** En atención al principio de finalidad se considera que una finalidad está determinada cuando haya sido expresada con claridad, sin lugar a confusión y cuando de manera objetiva se especifica el objeto que tendrá el tratamiento de los datos personales. Tratándose de banco de datos personales que contengan datos sensibles, su creación solo puede justificarse si su finalidad además de ser legítima, es concreta y acorde con las actividades o fines explícitos del titular del banco de datos personales. Los profesionales que realicen el tratamiento de algún dato personal, además de estar limitados por la finalidad de sus servicios, se encuentran obligados a guardar secreto profesional. **Artículo 9.- Principio de calidad**. En atención al principio de calidad, los datos contenidos en un banco de datos personales, deben ajustarse con precisión a la realidad. Se presume que los datos directamente facilitados por el titular de los mismos son exactos.

LOPDP	Reglamento de la ley No 29733, Ley de Protección de Datos Personales
en su relación con el responsable en cuanto a su uso posterior, la naturaleza de los datos personales, las consecuencias para los titulares del tratamiento ulterior previsto y la existencia de garantías adecuadas tanto en la operación de tratamiento original como en la operación de tratamiento ulterior prevista. **e) Pertinencia y minimización de datos personales.** Los datos personales deben ser pertinentes y estar limitados a lo estrictamente necesario para el cumplimiento de la finalidad del tratamiento. **f) Proporcionalidad del tratamiento. -** El tratamiento debe ser adecuado, necesario, oportuno, relevante y no excesivo con relación a las finalidades para las cuales hayan sido recogidos o a la naturaleza misma, de las categorías especiales de datos. **g) Confidencialidad. -** El tratamiento de datos personales debe concebirse sobre la base del debido sigilo y secreto, es decir, no debe tratarse o comunicarse para un fin distinto para el cual fueron recogidos, a menos que concurra una de las causales que habiliten un nuevo tratamiento conforme los supuestos de tratamiento legítimo señalados en esta ley. Para tal efecto, el responsable del tratamiento deberá adecuar las medidas técnicas organizativas para cumplir con este principio. **h) Calidad y exactitud. -** Los datos personales que sean objeto de tratamiento deben ser exactos, íntegros, precisos, completos, comprobables, claros; y, de ser el caso, debidamente actualizado; de tal forma que no se altere su veracidad. Se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan. En caso de tratamiento por parte de un encargado, la calidad y exactitud será obligación del responsable del tratamiento de datos personales. Siempre que el responsable del tratamiento haya adoptado todas las medidas razonables para que se supriman o rectifiquen sin dilación, no le será imputable la inexactitud de los datos personales, con respecto a los fines para los que se tratan, cuando los datos inexactos: a) Hubiesen sido obtenidos por el responsable directamente del titular.	**Artículo 10.- Principio de seguridad**. En atención al principio de seguridad, en el tratamiento de los datos personales deben adoptarse las medidas de seguridad que resulten necesarias a fi n de evitar cualquier tratamiento contrario a la Ley o al presente reglamento, incluyéndose en ellos a la adulteración, la pérdida, las desviaciones de información, intencionales o no, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.

LOPDP	Reglamento de la ley No 29733, Ley de Protección de Datos Personales
b) Hubiesen sido obtenidos por el responsable de un intermediario en caso de que las normas aplicables al sector de actividad al que pertenezca el responsable del tratamiento establecieran la posibilidad de intervención de un intermediario que recoja en nombre propio los datos de los afectados para su transmisión al responsable. c) Fuesen obtenidos de un registro público por el responsable. **i) Conservación.-** Los datos personales serán conservados durante un tiempo no mayor al necesario para cumplir con la finalidad de su tratamiento. Para garantizar que los datos personales no se conserven más tiempo del necesario, el responsable del tratamiento establecerá plazos para su supresión o revisión periódica. La conservación ampliada de tratamiento de datos personales únicamente se realizará con fines de archivo en interés público, fines de investigación científica, histórica o estadística, siempre y cuando se establezcan las garantías de seguridad y protección de datos personales, oportunas y necesarias, para salvaguardar los derechos previstos en esta norma. **j) Seguridad de datos personales. -** Los responsables y encargados de tratamiento de los datos personales deberán implementar todas las medidas de seguridad adecuadas y necesarias, entendiéndose por tales las aceptadas por el estado de la técnica, sean estas organizativas, técnicas o de cualquier otra índole, para proteger los datos personales, frente a cualquier riesgo, amenaza, vulnerabilidad, atendiendo a la naturaleza de los datos de carácter personal, al ámbito y el contexto. personales deberá acreditar el haber implementado mecanismos para la protección de datos personales; es decir, el cumplimiento de los principios, derechos y obligaciones establecidos en la presente Ley, para lo cual, además de lo establecido en la normativa aplicable, podrá valerse de estándares, mejores prácticas, esquemas de auto y coregulación, códigos de protección, sistemas de certificación, sellos de protección de datos personales o cualquier otro mecanismo que se determine adecuado a los fines, la naturaleza del dato personal o el riesgo del tratamiento.	

LOPDP	Reglamento de la ley No 29733, Ley de Protección de Datos Personales
El responsable del tratamiento de datos personales está obligado a rendir cuentas sobre el tratamiento al titular y a la Autoridad de Protección de Datos Personales. El responsable del tratamiento de datos personales deberá evaluar y revisar los mecanismos que adopte para cumplir con el principio de responsabilidad de forma continua y permanente, con el objeto de mejorar su nivel de eficacia en cuanto a la aplicación de la presente Ley. **l) Aplicación favorable al titular. -** En caso de duda sobre el alcance de las disposiciones del ordenamiento jurídico o contractuales, aplicables a la protección de datos personales, los funcionarios judiciales y administrativos las interpretarán y aplicarán en el sentido más favorable al titular de dichos datos. **m) Independencia del control. -** Para el efectivo ejercicio del derecho a la protección de datos personales, y en cumplimiento de las obligaciones de protección de los derechos que tiene el Estado, la Autoridad de Protección de Datos deberá ejercer un control independiente, imparcial y autónomo, así como llevar a cabo las respectivas acciones de prevención, investigación y sanción.	
Art. 11.- Normativa especializada. - Los datos personales cuyo tratamiento se encuentre regulado en normativa especializada en materia de ejercicio de la libertad de expresión, sectores regulados por normativa específica, gestión de riesgos, desastres naturales, seguridad nacional y defensa del Estado; y, los datos personales que deban proporcionarse a autoridades administrativas o judiciales en virtud de solicitudes y órdenes amparadas en competencias atribuidas en la normativa vigente, estarán sujetos a los principios establecidos en sus propias normas y los principios establecidos en esta Ley, en los casos que corresponda y sea de aplicación favorable. En todo caso deberá darse cumplimiento a los estándares internacionales en la materia de derechos humanos y a los principios de esta ley, y como mínimo a los criterios de legalidad, proporcionalidad y necesidad.	**NO EXISTE ARTÍCULO SUMILAR**

LOPDP	Reglamento de la ley No 29733, Ley de Protección de Datos Personales
Art. 12.- Derecho a la información. – El titular de datos personales tiene derecho a ser informado conforme los principios de lealtad y transparente por cualquier medio sobre: 1) Los fines del tratamiento; 2) La base legal para el tratamiento; 3) Tipos de tratamiento; 4) Tiempo de conservación; 5) La existencia de una base de datos en la que constan sus datos personales; 6) El origen de los datos personales cuando no se hayan obtenido directamente del titular; 7) Otras finalidades y tratamientos ulteriores; 8) Identidad y datos de contacto del responsable del tratamiento de datos personales, que incluirá: dirección del domicilio legal, número de teléfono y correo electrónico; 9) Cuando sea del caso, identidad y datos de contacto del delegado de protección de datos personales, que incluirá: dirección domiciliaria, número de teléfono y correo electrónico; 10) Las transferencias o comunicaciones, nacionales o internacionales, de datos personales que pretenda realizar, incluyendo los destinatarios y sus clases, así como las finalidades que motivan la realización de estas y las garantías de protección establecidas; 11) Las consecuencias para el titular de los datos personales de su entrega o negativa a ello; 12) El efecto de suministrar datos personales erróneos o inexactos; 13) La posibilidad de revocar el consentimiento; 14) La existencia y forma en que pueden hacerse efectivos sus derechos de acceso, eliminación, rectificación y actualización, oposición, anulación, limitación del tratamiento y a no ser objeto de una decisión basada únicamente en valoraciones automatizadas. 15) Los mecanismos para hacer efectivo su derecho a la portabilidad, cuando el titular lo solicite;	**Capítulo II** **Disposiciones especiales** **Artículo 60.- Derecho a la información.** El titular de datos personales tiene derecho, en vía de acceso, a que se le brinde toda la información señalada en el artículo 18 de la Ley y el numeral 4 del artículo 12 del presente reglamento. La respuesta contendrá los extremos previstos en los artículos citados en el párrafo anterior, salvo que el titular haya solicitado la información referida sólo a alguno de ellos. Será de aplicación para la respuesta al ejercicio del derecho a la información, en lo que fuere pertinente, lo establecido en los artículos 62 y 63 del presente reglamento.

LOPDP	Reglamento de la ley No 29733, Ley de Protección de Datos Personales
16) Dónde y cómo realizar sus reclamos ante el responsable del tratamiento de datos personales *y* la Autoridad de Protección de Datos Personales, y; 17) La existencia de valoraciones y decisiones automatizadas, incluida la elaboración de perfiles. En el caso que los datos se obtengan directamente del titular, la información deberá ser comunicada de forma previa a este, es decir, en el momento mismo de la recogida del dato personal. Cuando los datos personales no se obtuvieren de forma directa del titular o fueren obtenidos de una fuente accesible al público, el titular deberá, ser informado dentro de los siguientes treinta (30) días o al momento de la primera comunicación con el titular, cualquiera de las dos circunstancias que ocurra primero. Se le deberá proporcionar información expresa, inequívoca, transparente, inteligible, concisa, precisa y sin barreras técnicas. La información proporcionada al titular podrá transmitirse de cualquier modo comprobable en un lenguaje claro, sencillo y de fácil comprensión, de preferencia propendiendo a que pueda ser accesible en la lengua de su elección. En el caso de productos o servicios dirigidos, utilizados o que pudieran ser utilizados por niñas, niños y adolescentes, la información a la que hace referencia el presente arríenlo será, proporcionada a su representante legal conforme a lo dispuesto en la presente Ley.	
Art. 13.- Derecho de acceso. - El titular tiene derecho a conocer y a obtener, gratuitamente, del responsable de tratamiento acceso a todos sus datos personales y a la información detallada en el artículo precedente, sin necesidad de presentar justificación alguna. El responsable del tratamiento de datos personales deberá establecer métodos razonables que permitan el ejercicio de este derecho, el cual deberá ser atendido dentro del plazo de quince (15) días El derecho de acceso no podrá ejercerse de forma tal que constituya abuso del derecho.	**Artículo 61.- Derecho de acceso**. Sin perjuicio de lo señalado en el artículo 19 de la Ley, el titular de los datos personales tiene derecho a obtener del titular del banco de datos personales o responsable del tratamiento la información relativa a sus datos personales, así como a todas las condiciones y generalidades del tratamiento de los mismos.

LOPDP	Reglamento de la ley No 29733, Ley de Protección de Datos Personales
Art. 14.- Derecho de rectificación y actualización. – El titular tiene el derecho a obtener del responsable del tratamiento la rectificación y actualización de sus datos personales inexactos o incompletos. Para tal efecto, el titular deberá presentar los justificativos del caso, cuando sea pertinente. El responsable de tratamiento deberá atender el requerimiento en un plazo de quince (15) días y en este mismo plazo, deberá informar al destinatario de los datos, de ser el caso, sobre la rectificación, a fin de que lo actualice.	**Artículo 64.- Actualización.** Es derecho del titular de datos personales, en vía de rectificación, actualizar aquellos datos que han sido modificados a la fecha del ejercicio del derecho. La solicitud de actualización deberá señalar a qué datos personales se refiere, así como la modificación que haya de realizarse en ellos, acompañando la documentación que sustente la procedencia de la actualización solicitada. **Artículo 65.- Rectificación.** Es derecho del titular de datos personales que se modifiquen los datos que resulten ser inexactos, erróneos o falsos. La solicitud de rectificación deberá indicar a qué datos personales se refiere, así como la corrección que haya de realizarse en ellos, acompañando la documentación que sustente la procedencia de la rectificación solicitada.
Art. 15.- Derecho de eliminación. El titular tiene derecho a que el responsable del tratamiento suprima sus datos personales, cuando: 1) El tratamiento no cumpla con los principios establecidos en la presente ley; 2) El tratamiento no sea necesario o pertinente para el cumplimiento de la finalidad; 3) Los datos personales hayan cumplido con la finalidad para la cual fueron recogidos o tratados; 4) Haya vencido el plazo de conservación de los datos personales; 5) El tratamiento afecte derechos fundamentales o libertades individuales; 6) Revoque el consentimiento prestado o señale no haberlo otorgado para uno o varios fines específicos, sin necesidad de que medie justificación alguna; o, 7) Exista obligación legal. El responsable del tratamiento de datos personales implementará métodos y técnicas orientadas a eliminar, hacer ilegible, o dejar irreconocibles de forma definitiva y segura los datos personales. Esta obligación la deberá cumplir en el plazo de quince (15) días de recibida la solicitud por parte del titular y será gratuito.	**Artículo 67.- Supresión o cancelación**. El titular de los datos personales podrá solicitar la supresión o cancelación de sus datos personales de un banco de datos personales cuando éstos hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hayan sido recopilados, cuando hubiere vencido el plazo establecido para su tratamiento, cuando ha revocado su consentimiento para el tratamiento y en los demás casos en los que no están siendo tratados conforme a la Ley y al presente reglamento. La solicitud de supresión o cancelación podrá referirse a todos los datos personales del titular contenidos en un banco de datos personales o sólo a alguna parte de ellos. Dentro de lo establecido por el artículo 20 de la Ley y el numeral 3) del artículo 2 del presente reglamento, la solicitud de supresión implica el cese en el tratamiento de los datos personales a partir de un bloqueo de los mismos y su posterior eliminación. **Artículo 68.- Comunicación de la supresión o cancelación.** El titular del banco de datos personales o responsable del tratamiento deberá documentar ante el titular de los datos personales haber cumplido con lo solicitado e indicar las transferencias de los datos suprimidos, identificando a quién o a quiénes fueron transferidos, así como la comunicación de la supresión correspondiente. **Artículo 69.- Improcedencia de la supresión o cancelación.** La supresión no procederá cuando los datos personales deban ser conservados en virtud de razones históricas , estadísticas o científicas de acuerdo con la legislación aplicable o,

LOPDP	Reglamento de la ley No 29733, Ley de Protección de Datos Personales
	en su caso, en las relaciones contractual es entre el responsable y el titular de los datos personales, que justifiquen el tratamiento de los mismos.
	Artículo 70.- Protección en caso de denegatoria de supresión o cancelación.
	Siempre que sea posible, según la naturaleza de las razones que sustenten la denegatoria prevista en el párrafo precedente, se deberán emplear medios de disociación o anonimización para continuar el tratamiento.
Art. 16.- Derecho de oposición. – El titular tiene el derecho a oponerse o negarse al tratamiento de sus datos personales, en los siguientes casos:	**Artículo 71.- Oposición.**
1) No se afecten derechos y libertades fundamentales de terceros, la ley se lo permita y no se trate de información pública, de interés público o cuyo tratamiento está ordenado por la ley.	El titular de datos personales tiene derecho a que no se lleve a cabo el tratamiento de sus datos personales o se cese en el mismo, cuando no hubiere prestado su consentimiento para su recopilación por haber sido tomados de fuente de acceso al público.
2) El tratamiento de datos personales tenga por objeto la mercadotecnia directa; el interesado tendrá derecho a oponerse en todo momento al tratamiento de los datos personales que le conciernan, incluida la elaboración de perfiles; en cuyo caso los datos personales dejarán de ser tratados para dichos fines.	Aun cuando hubiera prestado consentimiento, el titular de datos personales tiene derecho a oponerse al tratamiento de sus datos, si acredita la existencia de motivos fundados y legítimos relativos a una concreta situación personal que justifiquen el ejercicio de este derecho.
3) Cuando no sea necesario su consentimiento para el tratamiento como consecuencia de la concurrencia de un interés legítimo, previsto en el artículo 7, y se justifique en una situación concreta personal del titular, siempre que una ley no disponga lo contrario.	En caso que la oposición resulte justificada el titular del banco de datos personales o responsable de su tratamiento deberá proceder al cese del tratamiento que ha dado lugar a la oposición.
El responsable de tratamiento dejará de tratar los datos personales en estos casos, salvo que acredite motivos legítimos e imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del titular, o para la formulación, el ejercicio o la defensa de reclamaciones.	
Esta solicitud deberá ser atendida dentro del plazo de quince (15) días	
Art. 17.- Derecho a la portabilidad. - El titular tiene el derecho a recibir del responsable del tratamiento, sus datos personales en un formato compatible, actualizado, estructurado, común, interoperable y de lectura mecánica, preservando sus características; o a transmitirlos a otros responsables. La Autoridad de Protección de Datos Personales deberá dictar la normativa para el ejercicio del derecho a la portabilidad.	**Artículo 33.- Tratamiento de los datos personales**
	Por medios tecnológicos tercerizados. El tratamiento de datos personales por medios tecnológicos tercerizados, entre los que se encuentran servicios, aplicaciones, infraestructura, entre otros, está referido a aquellos, en los que el procesamiento es automático, sin intervención humana.
	Para los casos en los que en el tratamiento exista intervención humana se aplican los artículos 37 y 38.

LOPDP	Reglamento de la ley No 29733, Ley de Protección de Datos Personales
El titular podrá solicitar que el responsable del tratamiento realice la transferencia o comunicación de sus datos personales a otro responsable del tratamiento en cuanto fuera técnicamente posible y sin que el responsable pueda aducir impedimento de cualquier orden con el fin de ralentizar el acceso, la transmisión o reutilización de datos por parte del titular o de otro responsable del tratamiento. Luego de completada la transferencia de datos, el responsable que lo haga procederá a su eliminación, salvo que el titular disponga su conservación. El responsable que ha recibido la información asumirá las responsabilidades contempladas en esta Ley. Para que proceda el derecho a la portabilidad de datos es necesario que se produzca al menos una de las siguientes condiciones; 1) Que el titular haya otorgado su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos. La transferencia o comunicación se hará entre responsables del tratamiento de datos personales cuando la operación sea técnicamente posible; en caso contrario los datos deberán ser transmitidos directamente al titular. 2) Que el tratamiento se efectúe por medios automatizados; 3) Que se trate de un volumen relevante de datos personales, según los parámetros definidos en el reglamento de la presente ley; o, 4) Que el tratamiento sea necesario para el cumplimiento de obligaciones y el ejercicio de derechos del responsable o encargado del tratamiento de datos personales, o del titular en el ámbito del derecho laboral y seguridad social Esta transferencia o comunicación debe ser económica y financieramente eficiente, expedita y sin trabas. No procederá este derecho cuando se trate de información inferida, derivada, creada, generada u obtenida a partir del análisis o tratamiento efectuado por el responsable del tratamiento de datos personales con base en los datos personales proporcionados por el titular, como es el caso de los datos personales que hubieren sido sometidos a un proceso de personalización, recomendación, categorización o creación de perfiles.	El tratamiento de datos personales por medios tecnológicos tercerizados, sea completo o parcial, podrá ser contratado por el responsable del tratamiento de datos personales siempre y cuando para la ejecución de aquel se garantice el cumplimiento de lo establecido en la Ley y el presente reglamento **Artículo 34.- Criterios a considerar para el tratamiento de datos personales por medios tecnológicos tercerizados**. Al realizar el tratamiento de los datos personales por medios tecnológicos tercerizados se deberá considerar como prestaciones mínimas las siguientes: 1. Informar con transparencia las subcontrataciones que involucren la información sobre la que presta el servicio. 2. No incluir condiciones que autoricen o permitan al prestador asumir la titularidad sobre los bancos de datos personales tratados en la tercerización. 3. Garantizar la confidencialidad respecto de los datos personales sobre los que preste el servicio. 4. Mantener el control, las decisiones y la responsabilidad sobre el proceso mediante el cual se realiza el tratamiento de los datos personales. 5. Garantizar la destrucción o la imposibilidad de acceder a los datos personales después de concluida la prestación. **Artículo 37.- Tratamiento a través de subcontratación**. El tratamiento de datos personales puede realizarse por un tercero diferente al encargado del tratamiento, a través de un convenio o contrato entre estos dos. Para este supuesto se requerirá de manera previa una autorización por parte del titular del banco de datos personales o responsable del tratamiento. Dicha autorización se entenderá también concedida si estaba prevista en el instrumento jurídico mediante el cual se formalizó la relación entre el responsable del tratamiento y el encargado del mismo. El tratamiento que haga el subcontratista se realizará en nombre y por cuenta del responsable del tratamiento, pero la carga de probar la autorización le corresponde al encargado del tratamiento. **Artículo 38.- Responsabilidad del tercero subcontratado.** La persona natural o jurídica subcontratada asume las mismas obligaciones que se establezcan para el encargado del tratamiento en la Ley, el presente reglamento y demás

LOPDP	Reglamento de la ley No 29733, Ley de Protección de Datos Personales
Art. 18.- Excepciones a los derechos de rectificación, actualización, eliminación, oposición, anulación y portabilidad. – Excepciones a los derechos de rectificación, actualización, eliminación, oposición, anulación y portabilidad. No proceden los derechos de rectificación, actualización, eliminación, oposición, anulación y portabilidad, en los siguientes casos; 1) Si el solicitante no es el titular de los datos personales o su representante legal no se encuentre debidamente acreditado; 2) Cuando los datos son necesarios para el cumplimiento de una obligación legal o contractual; 3) Cuando los datos son necesarios para el cumplimiento de una orden judicial, resolución o mandato motivado de autoridad pública competente; 4) Cuando los datos son necesarios para la formulación, ejercicio o defensa de reclamos o recursos; 5) Cuando se pueda causar perjuicios a derechos o afectación a intereses legítimos de terceros y ello sea acreditado por el responsable de la base de datos al momento de dar respuesta al titular a su solicitud de ejercicio del derecho respectivo; 6) Cuando se pueda obstaculizar actuaciones judiciales o administrativas en curso, debidamente notificadas; 7) Cuando los datos son necesarios para ejercer el derecho a la libertad de expresión y opinión; 8) Cuando los datos son necesarios para proteger el interés vital del interesado o de otra persona natural; 9) En los casos en los que medie el interés público, sujeto al cumplimiento de los estándares internacionales de derechos humanos aplicables a la	disposiciones aplicables. Sin embargo, asumirá las obligaciones del titular del banco de datos personales o encargado del tratamiento cuando: 1. Destine o utilice los datos personales con una finalidad distinta a la autorizada por el titular del banco de datos o responsable del tratamiento; o 2. Efectúe una transferencia, incumpliendo las instrucciones del titular del banco de datos personales, aun cuando sea para la conservación de dichos datos. **Artículo 59.- Denegación parcial o total ante el ejercicio de un derecho** La respuesta total o parcialmente negativa por parte del titular del banco de datos personales o del responsable del tratamiento ante la solicitud de un derecho del titular de datos personales, debe estar debidamente justificada y debe señalar el derecho que le asiste al mismo para recurrir ante la Dirección General de Protección de Datos Personales en vía de reclamación, en los términos del artículo 24 de la Ley y del presente reglamento

LOPDP	Reglamento de la ley No 29733, Ley de Protección de Datos Personales
materia, al cumplimiento de los principios de esta ley y a los criterios de legalidad, proporcionalidad y necesidad; 10) En el tratamiento de datos personales que sean necesarios para el archivo de información que constituya patrimonio del Estado, investigación científica, histórica o estadística. **Art. 19.- Derecho a la suspensión del tratamiento. –** El titular tendrá derecho a obtener del responsable del tratamiento la suspensión del tratamiento de los datos cuando se cumpla alguna de las condiciones siguientes: 1) Cuando el titular impugne la exactitud de los datos personales, mientras el responsable de tratamiento verifica la exactitud de los mismos; 2) El tratamiento sea ilícito *y* el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso; 3) El responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones; y. 4) Cuando el interesado se haya opuesto al tratamiento en virtud del artículo 31 de la presente ley; mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado. De existir negativa por parte del responsable o encargado del tratamiento de datos personales^ y el titular recurra por dicha decisión ante la Autoridad de Protección de Datos Personales, esta suspensión se extenderá hasta la resolución del procedimiento administrativo. Cuando el titular impugne la exactitud de los datos personales, mientras el responsable de tratamiento verifica la exactitud de los mismos, deberá colocarse en la base de datos, en donde conste 1a información impugnada, que ésta ha sido objeto de inconformidad por parte del titular. El responsable de tratamiento podrá tratar los datos personales, que han sido objeto del ejercicio del presente derecho por parte del titular, únicamente, en los siguientes supuestos; para la formulación, el ejercicio o la defensa de reclamaciones; con el objeto de proteger los derechos de otra persona natural o jurídica o por razones de interés público importante.	**Artículo 67.- Supresión o cancelación.** El titular de los datos personales podrá solicitar la supresión o cancelación de sus datos personales de un banco de datos personales cuando éstos hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hayan sido recopilados, cuando hubiere vencido el plazo establecido para su tratamiento, cuando ha revocado su consentimiento para el tratamiento y en los demás casos en los que no están siendo tratados conforme a la Ley y al presente reglamento. La solicitud de supresión o cancelación podrá referirse a todos los datos personales del titular contenidos en un banco de datos personales o sólo a alguna parte de ellos. Dentro de lo establecido por el artículo 20 de la Ley y el numeral 3) del artículo 2 del presente reglamento, la solicitud de supresión implica el cese en el tratamiento de los datos personales a partir de un bloqueo de los mismos y su posterior eliminación.

LOPDP	Reglamento de la ley No 29733, Ley de Protección de Datos Personales
Art. 25.- Categorías especiales de datos personales. - Se considerarán categorías especiales de datos personales, los siguientes: a) Datos sensibles; b) Datos de niñas, niños y adolescentes: c) Datos de salud; y, d) Datos de personas con discapacidad y de sus sustitutos, relativos a la discapacidad.	**Capítulo IV** **Tratamientos especiales de datos personales** **Artículo 27.- Tratamiento de los datos personales de menores**. Para el tratamiento de los datos personales de un menor de edad, se requerirá el consentimiento de los titulares de la patria potestad o tutores, según corresponda.
Art. 26.- Tratamiento de datos sensibles. - Queda prohibido el tratamiento de datos personales sensibles salvo que concurra alguna de las siguientes circunstancias: a) El titular haya dado su consentimiento explícito para el tratamiento de sus datos personales, especificándose claramente sus fines. b) El tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del titular en el ámbito del Derecho laboral y de la seguridad y protección social. c) El tratamiento es necesario para proteger intereses vitales del titular o de otra persona natural, en el supuesto de que el titular no esté capacitado, física o jurídicamente, para dar su consentimiento. d) El tratamiento se refiere a datos personales que el titular ha hecho manifiestamente públicos. e) El tratamiento se lo realiza por orden de autoridad judicial. f) El tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del titular. g) Cuando el tratamiento de los datos de salud se sujete a las disposiciones contenidas en la presente ley.	**Artículo 14.- Consentimiento y datos sensibles.** Tratándose de datos sensibles, el consentimiento debe ser otorgado por escrito, a través de su firma manuscrita, firma digital o cualquier otro mecanismo de autenticación que garantice la voluntad inequívoca del titular.
Art. 27.- Datos personales de personas fallecidas. -Los titulares de derechos sucesorios de las personas fallecidas, podrán dirigirse al responsable del tratamiento de datos personales con el objeto de solicitar el acceso, rectificación y actualización o eliminación de los datos personales del causante, siempre que el titular de los datos no haya, en vida, indicado otra	Al respecto, debemos manifestar que la Ley N° 29733, Ley de Protección de Datos Personales (en adelante, "LPDP"), define al titular de datos personales como la "persona natural a quien corresponde los datos personales". En tal sentido, habiendo señalado que la muerte le pone fin a la persona y considerando que la mencionada ley sólo tutela los datos personales de las personas naturales, resulta evidente que el derecho a la

LOPDP	Reglamento de la ley No 29733, Ley de Protección de Datos Personales
utilización o destino para sus datos. Las personas o instituciones que la o el fallecido haya designado expresamente para ello, podrán también solicitar con arreglo a las instrucciones recibidas, el acceso a los datos personales de éste; y, en su caso, su rectificación, actualización o eliminación. En caso de fallecimiento de niñas, niños, adolescentes o personas que la ley reconozca come incapaces, las facultades de acceso, rectificación, actualización o eliminación, podrán ser ejercidas por quien hubiese sido su último representante legal. El Reglamento a la presente ley establecerá los mecanismos para el ejercicio de las facultades enunciadas en el presente artículo.	protección de datos personales desaparece por la muerte, por lo que los tratamientos de datos de personas fallecidas no podrían considerarse comprendidos dentro del ámbito de aplicación de la LPDP.
Art. 33.- Transferencia o comunicación de datos personales. Los datos personales podrán transferirse o comunicarse a terceros cuando se realice para el cumplimiento de fines directamente relacionados con las funciones legítimas del responsable y del destinatario, cuando la transferencia se encuentre configurada dentro de una de las causales de legitimidad establecidas en esta Ley, y se cuente, además, con el consentimiento del titular. Se entenderá que el consentimiento es informado cuando para la transferencia o comunicación de datos personales el Responsable del tratamiento haya entregado información suficiente al titular que le permita conocer la finalidad a que se destinarán sus datos y el tipo de actividad del tercero a quien se pretende transferir o comunicar dichos datos.	**Artículo 18.- Disposiciones generales.** La transferencia de datos personales implica la comunicación de datos personales dentro o fuera del territorio nacional realizada a persona distinta al titular de los datos personales, al encargado del banco de datos personales o al encargado del tratamiento de datos personales. Se denomina flujo transfronterizo de datos personales a la transferencia de datos personales fuera del territorio nacional. Aquél a quien se transfieran los datos personales se obliga, por el solo hecho de la transferencia, a la observancia de las disposiciones de la Ley y del presente reglamento.
Art. 34.- Acceso a datos personales por parte del encargado- No se considerará transferencia o comunicación en el caso de que el encargado acceda a datos personales para la prestación de un servicio al responsable del tratamiento de datos personales. El tercero que ha accedido legítimamente a datos personales en estas consideraciones, será considerado encargado del tratamiento. El tratamiento de datos personales realizado por el encargado deberá estar regulado por un contrato, en el que se establezca de manera clara y precisa que el encargado del tratamiento de datos personales tratará únicamente los mismos conforme las instrucciones del responsable y que no los utilizará para	**Artículo 36.- Prestación de servicios o tratamiento por encargo.** Para efectos de la Ley, la entrega de datos personales del titular del banco de datos personales al encargado no constituye transferencia de datos personales. El encargado del banco de datos personales se encuentra prohibido de transferir a terceros los datos personales objeto de la prestación de servicios de tratamiento, a menos que el titular del banco de datos personales que le encargó el tratamiento lo haya autorizado y el titular del dato personal haya brindado su consentimiento, en los supuestos que dicho consentimiento sea requerido conforme a Ley. El plazo para la conservación de los datos será de dos (2) años contado desde la finalización del último encargo realizado.

LOPDP	Reglamento de la ley No 29733, Ley de Protección de Datos Personales
finalidades diferentes a las señaladas en el contrato, ni que los transferirá o comunicará ni siquiera para su conservación a otras personas. Una vez que se haya cumplido la prestación contractual, los datos personales deberán ser destruidos o devueltos al responsable del tratamiento de datos personales bajo la supervisión de la Autoridad de Protección de Datos Personales.	Lo dispuesto en el presente artículo será aplicable, en lo que corresponda, a la subcontratación de la prestación de servicios de tratamiento de datos personales.
Art. 35.- Acceso a datos personales por parte de terceros. - No se considerará transferencia o comunicación cuando el acceso a datos personales por un tercero sea necesario para la prestación de un servicio al responsable del tratamiento de datos personales. El tercero que ha accedido a datos personales en estas condiciones debió hacerlo legítimamente. El tratamiento de datos personales realizado por terceros deberá estar regulado por un contrato, en el que se establezca de manera clara y precisa que el encargado del tratamiento de datos personales tratará únicamente los mismos conforme las instrucciones del responsable y que no los utilizará para finalidades diferentes a las Señaladas en el contrato, ni que los transferirá o comunicará ni siquiera para su ¡conservación a otras personas. Una vez que se haya cumplido la prestación contractual, los datos personales deberán ser destruidos o devueltos al responsable del tratamiento de datos personales bajo la supervisión de la autoridad de protección de datos personales. El tercero será responsable de las infracciones derivadas del incumplimiento de las condiciones de tratamiento de datos personales establecidas en la presente ley.	**Artículo 37.- Tratamiento a través de subcontratación.** El tratamiento de datos personales puede realizarse por un tercero diferente al encargado del tratamiento, a través de un convenio o contrato entre estos dos. Para este supuesto se requerirá de manera previa una autorización por parte del titular del banco de datos personales o responsable del tratamiento. Dicha autorización se entenderá también concedida si estaba prevista en el instrumento jurídico mediante el cual se formalizó la relación entre el responsable del tratamiento y el encargado del mismo. El tratamiento que haga el subcontratista se realizará en nombre y por cuenta del responsable del tratamiento, pero la carga de probar la autorización le corresponde al encargado del tratamiento. **Artículo 38.- Responsabilidad del tercero subcontratado.** La persona natural o jurídica subcontratada asume las mismas obligaciones que se establezcan para el encargado del tratamiento en la Ley, el presente reglamento y demás disposiciones aplicables. Sin embargo, asumirá las obligaciones del titular del banco de datos personales o encargado del tratamiento cuando: 1. Destine o utilice los datos personales con una finalidad distinta a la autorizada por el titular del banco de datos o responsable del tratamiento; o 2. Efectúe una transferencia, incumpliendo las instrucciones del titular del banco de datos personales, aun cuando sea para la conservación de dichos datos.
Art. 36.- Excepciones de consentimiento para la transferencia o comunicación de datos personales. - No es necesario contar con el consentimiento del titular para la transferencia o comunicación de datos personales, en los siguientes supuestos: 1) Cuando los datos han sido recogidos de fuentes accesibles al público;	**Capítulo II** **Limitaciones al consentimiento** **Artículo 17.- Fuentes accesibles al público.** Para los efectos del artículo 2, inciso 9) de la Ley, se considerarán fuentes accesibles al público, con independencia de que el acceso requiera contraprestación, las siguientes:

LOPDP	Reglamento de la ley No 29733, Ley de Protección de Datos Personales
2) Cuando el tratamiento responda a la libre y legítima aceptación de una relación Página 20 de 40 jurídica entre el responsable de tratamiento y el titular, cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con base de datos. En este caso la transferencia o comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique; 3) Cuando los datos personales deban proporcionarse a autoridades administrativas o judiciales en virtud de solicitudes y órdenes amparadas en competencias atribuidas en la norma vigente; 4) Cuando la comunicación se produzca entre Administraciones Públicas y tenga por objeto el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre y cuando dichos datos se encuentren debidamente disociados o a lo menos anonimizados, y, 5) Cuando la comunicación de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que implique intereses vitales de su titular y este se encontrare impedido de otorgar su consentimiento. 6) Cuando la comunicación de datos de carácter personal relativos a la salud sea necesaria para realizar los estudios epidemiológicos de interés público, dando cumplimiento a los estándares internacionales en la materia de derechos humanos, y como mínimo a los criterios de legalidad, proporcionalidad y necesidad. El tratamiento deberá ser de preferencia anonimizado, y en todo caso agregado» una vez pasada la urgencia de interés público. Cuando sea requerido el consentimiento del titular para que sus datos personales sean comunicados a un tercero, este puede revocarlo en cualquier momento, sin necesidad de que medie justificación alguna. La presente ley obligatoriamente debe ser aplicada por el destinatario, por el solo hecho de la comunicación de los datos; a menos que estos hayan sido anonimizados o sometidos a un proceso de **Capítulo VI** **SEGURIDAD DE DATOS PERSONALES** **Ar. 37.- Seguridad de datos personales**.	1. Los medios de comunicación electrónica, óptica y de otra tecnología, siempre que el lugar en el que se encuentren los datos personales esté concebido para facilitar información al público y esté abierto a la consulta general. 2. Las guías telefónicas, independientemente del soporte en el que estén a disposición y en los términos de su regulación específica. 3. Los diarios y revistas independientemente del soporte en el que estén a disposición y en los términos de su regulación específica. 4. Los medios de comunicación social. 5. Las listas de personas pertenecientes a grupos profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección postal, número telefónico, número de fax, dirección de correo electrónico y aquellos que establezcan su pertenencia al grupo. En el caso de colegios profesionales, podrán indicarse además los siguientes datos de sus miembros: número de colegiatura, fecha de incorporación y situación gremial en relación al ejercicio profesional. 6. Los repertorios de jurisprudencia, debidamente anonimizados. 7. Los Registros Públicos administrados por la Superintendencia Nacional de Registros Públicos - SUNARP, así como todo otro registro o banco de datos calificado como público conforme a ley. 8. Las entidades de la Administración Pública, en relación a la información que deba ser entregada en aplicación de la Ley Nº 27806, Ley de Transparencia y Acceso a la Información Pública. Lo dispuesto en el numeral precedente no quiere decir que todo dato personal contenido en información administrada por las entidades sujetas a la Ley de Transparencia y Acceso a la Información Pública sea considerado información pública accesible. La evaluación del acceso a datos personales en posesión de entidades de administración pública se hará atendiendo a las circunstancias de cada caso concreto. El tratamiento de los datos personales obtenidos a través de fuentes de acceso público deberá respetar los principios establecidos en la Ley y en el presente reglamento. **Capítulo V** **Medidas de seguridad** **Artículo 39.- Seguridad para el tratamiento de la información digital.**

LOPDP	Reglamento de la ley No 29733, Ley de Protección de Datos Personales
El responsable o encargado del tratamiento de datos personales según sea el caso, deberá sujetarse al principio de seguridad de datos personales, para lo cual deberá tomar en cuenta las categorías y volumen de datos personales, el estado de la técnica, mejores prácticas de seguridad integral y los costos de aplicación de acuerdo a la naturaleza, alcance, contexto y los fines del tratamiento, así como identificar la probabilidad de riesgos, El responsable o encargado del tratamiento de datos personales, deberá implementar un proceso de verificación, evaluación y valoración continua y permanente de la eficiencia, eficacia y efectividad de las medidas de carácter técnico, organizativo y de cualquier otra índole, implementadas con el objeto de garantizar y mejorar la seguridad del tratamiento de datos personales, El responsable o encargado del tratamiento de datos personales deberá evidenciar que las medidas adoptadas e implementadas mitiguen de forma adecuada los riesgos identificados Entre otras medidas, se podrán incluir las siguientes; 1) Medidas de anonimización, seudonomización o cifrado de datos personales; 2) Medidas dirigidas a mantener la confidencialidad, integridad y disponibilidad permanentes de los sistemas y servicios del tratamiento de datos personales y el acceso a los datos personales, de forma rápida en caso de incidentes; y 3) Medidas dirigidas a mejorar la resiliencia técnica, física, administrativa, y jurídica. 4) Los responsables y encargados del tratamiento de datos personales, podrán acogerse a estándares internacionales para una adecuada gestión de riesgos enfocada a Ja protección de derechos y libertades, así como para la implementación y manejo de sistemas de seguridad de la información o a códigos de conducta reconocidos y autorizados por la Autoridad de Protección de Datos Personales.	Los sistemas informáticos que manejen bancos de datos personales deberán incluir en su funcionamiento: 1. El control de acceso a la información de datos personales incluyendo la gestión de accesos desde el registro de un usuario, la gestión de los privilegios de dicho usuario, la identificación del usuario ante el sistema, entre los que se encuentran usuario-contraseña, uso de certificados digitales, tokens, entre otros, y realizar una verificación periódica de los privilegios asignados, los cuales deben estar definidos mediante un procedimiento documentado a fi n de garantizar su idoneidad. 2. Generar y mantener registros que provean evidencia sobre las interacciones con los datos lógicos, incluyendo para los fines de la trazabilidad, la información de cuentas de usuario con acceso al sistema, horas de inicio y cierre de sesión y acciones relevantes. Estos registros deben ser legibles, oportunos y tener un procedimiento de disposición, entre los que se encuentran el destino de los registros, una vez que éstos ya no sean útiles, su destrucción, transferencia, almacenamiento, entre otros. Asimismo, se deben establecer las medidas de seguridad relacionadas con los accesos autorizados a los datos mediante procedimientos de identificación y autenticación que garanticen la seguridad del tratamiento de los datos personales.
Art. 38.- Medidas de seguridad en el ámbito del sector público. – El mecanismo gubernamental de seguridad de la información deberá incluir las medidas que deban implementarse en el caso de tratamiento de datos	El reglamento no diferencia el sector público y el sector privado.

LOPDP	Reglamento de la ley No 29733, Ley de Protección de Datos Personales
personales para hacer frente a cualquier nesgo, amenaza., vulnerabilidad, accesos no autorizados, pérdidas, alteraciones, destrucción o comunicación accidental o ilícita en el tratamiento de los datos conforme al principio de seguridad de datos personales. El mecanismo gubernamental de seguridad de la información abarcará y aplicará a todas las instituciones del sector público, contenidas en el artículo 225 de la Constitución de la República de Ecuador, así como a terceros que presten servicios públicos mediante concesión, u otras figuras legalmente reconocidas. Estas, podrán incorporar medidas adicionales al mecanismo gubernamental de seguridad de la información.	
Art. 39.- Protección de datos personales desde el diseño y por defecto. – Se entiende a la protección de datos desde el diseño como el deber del responsable del tratamiento de tener en cuenta, en las primeras fases de concepción y diseño del proyecto, que determinados tipos de tratamientos de datos personales entrañan una serie de riesgos para los derechos de los titulares en atención al estado de la técnica, naturaleza y fines del tratamiento, para lo cual, implementará las medidas técnicas, organizativas y de cualquier otra Índole, con miras a garantizar el cumplimiento de las obligaciones en materia de protección de datos, en los términos del reglamento. La protección de datos por defecto hace referencia a que el responsable debe aplicar las medidas técnicas y organizativas adecuadas con miras a que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines del tratamiento, en los términos del reglamento.	**Artículo 39.- Seguridad para el tratamiento de la información digital.** Los sistemas informáticos que manejen bancos de datos personales deberán incluir en su funcionamiento: 1. El control de acceso a la información de datos personales incluyendo la gestión de accesos desde el registro de un usuario, la gestión de los privilegios de dicho usuario, la identificación del usuario ante el sistema, entre los que se encuentran usuario-contraseña, uso de certificados digitales, tokens, entre otros, y realizar una verificación periódica de los privilegios asignados, los cuales deben estar definidos mediante un procedimiento documentado a fi n de garantizar su idoneidad. 2. Generar y mantener registros que provean evidencia sobre las interacciones con los datos lógicos, incluyendo para los fines de la trazabilidad, la información de cuentas de usuario con acceso al sistema, horas de inicio y cierre de sesión y acciones relevantes. Estos registros deben ser legibles, oportunos y tener un procedimiento de disposición, entre los que se encuentran el destino de los registros, una vez que éstos ya no sean útiles, su destrucción, transferencia, almacenamiento, entre otros. Asimismo, se deben establecer las medidas de seguridad relacionadas con los accesos autorizados a los datos mediante procedimientos de identificación y autenticación que garanticen la seguridad del tratamiento de los datos personales.
Art. 40.- Análisis de riesgo, amenazas y vulnerabilidades Para el análisis de riesgos, amenazas y vulnerabilidades, el responsable y el encargado de tratamiento de los datos personales deberán utilizar una metodología que considere, entre otras; 1) Las particularidades del tratamiento;	**Artículo 40.- Conservación, respaldo y recuperación de los datos personales.** Los ambientes en los que se procese, almacene o transmita la información deberán ser implementados, con controles de seguridad apropiados, tomando como referencia las recomendaciones de seguridad física y ambiental recomendados en la “NTP ISO/IEC

LOPDP	Reglamento de la ley No 29733, Ley de Protección de Datos Personales
2) Las particularidades de las partes involucradas; y, 3) Las categorías y el volumen de datos personales objeto de tratamiento.	17799 EDI. Tecnología de la Información. Código de Buenas Prácticas para la Gestión de Seguridad de la Información." en la edición que se encuentre vigente. Adicionalmente, se deben contemplar los mecanismos de respaldo de seguridad de la información de la base de datos personales con un procedimiento que contemple la verificación de la integridad de los datos almacenados en el respaldo, incluyendo cuando sea pertinente, la recuperación completa ante una interrupción o daño, garantizando el retorno al estado en el que se encontraba al momento en que se produjo la interrupción o daño.
Art. 41.- Determinación de medidas de seguridad aplicables. Para determinar las medidas de seguridad, aceptadas por el estado de la técnica, a las que están obligadas el responsable y el encargado del tratamiento de los datos personales, se deberán tomar en consideración, entre otros: 1) Los resultados del análisis de riesgos, amenazas y vulnerabilidades; 2) La naturaleza de los datos personales; 3) Las características de las partes involucradas; y, 4) Los antecedentes de destrucción de datos personales, la pérdida, alteración, divulgación o impedimento de acceso a los mismos por parte del titular, sean accidentales e intencionales, por acción u omisión, así como los antecedentes de transferencia, comunicación o de acceso no autorizado o exceso de autorización de tales datos. El responsable y el encargado del tratamiento de datos personales deberán tomar las medidas adecuadas y necesarias, de forma permanente y continua, para evaluar, prevenir, impedir, reducir, mitigar y controlar los riesgos, amenazas y vulnerabilidades, incluidas las que conlleven un alto riesgo para los derechos y libertades del titular, de conformidad con la normativa que emita la Autoridad de Protección de Datos Personales.	**Artículo 40.- Conservación, respaldo y recuperación de los datos personales.** Los ambientes en los que se procese, almacene o transmita la información deberán ser implementados, con controles de seguridad apropiados, tomando como referencia las recomendaciones de seguridad física y ambiental recomendados en la "NTP ISO/IEC 17799 EDI. Tecnología de la Información. Código de Buenas Prácticas para la Gestión de Seguridad de la Información." en la edición que se encuentre vigente. Adicionalmente, se deben contemplar los mecanismos de respaldo de seguridad de la información de la base de datos personales con un procedimiento que contemple la verificación de la integridad de los datos almacenados en el respaldo, incluyendo cuando sea pertinente, la recuperación completa ante una interrupción o daño, garantizando el retorno al estado en el que se encontraba al momento en que se produjo la interrupción o daño.
Art. 43.- Notificación de vulneración de seguridad. – El responsable del tratamiento deberá notificar la vulneración de la seguridad de datos personales a la Autoridad de Protección de Datos Personales y la Agencia de Regulación y Control de las Telecomunicaciones, tan pronto sea posible, y a más tardar en el término de cinco (5) días después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la	**Artículo 40, que refiere a la aplicación de una norma ISO de seguridad.**

LOPDP	Reglamento de la ley No 29733, Ley de Protección de Datos Personales
seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la Autoridad de Protección de Datos no tiene lugar en el término de cinco (5) días, deberá ir acompañada de indicación de los motivos de la dilación. El encargado del tratamiento deberá notificar al responsable cualquier vulneración de la seguridad de datos personales tan pronto sea posible, y a más tardar dentro del término de dos (2) días contados a partir de la fecha en la que tenga conocimiento de ella.	
Art. 46.- Notificación de vulneración de seguridad al titular. - El responsable del tratamiento deberá notificar sin dilación la vulneración de seguridad de datos personales al titular cuando conlleve un riesgo a sus derechos fundamentales y libertades individuales, dentro del término de tres días contados a partir de la fecha en la que tuvo conocimiento del riesgo. No se deberá notificar la vulneración de seguridad de datos personales al titular en los siguientes casos: 1. Cuando el responsable del tratamiento haya adoptado medidas de protección técnicas organizativas o de cualquier otra índole apropiadas aplicadas a los datos personales afectados por la vulneración de seguridad que se pueda demostrar que son efectivas; 2. Cuando el responsable del tratamiento haya tomado medidas que garanticen que el riesgo para los derechos fundamentales y las libertades individuales del titular, no ocurrirá; y, 3. Cuando se requiera un esfuerzo desproporcionado para hacerlo; en cuyo caso, el responsable del tratamiento deberá realizar una comunicación pública a través de cualquier medio en la que se informe de la vulneración de seguridad de datos personales a los titulares. La procedencia de las excepciones de los numerales 1 y 2 deberá ser calificada por la Autoridad de Protección de Datos, una vez informada esta tan pronto sea posible, y en cualquier caso dentro de los plazos contemplados en el Articulo 43. La notificación al titular del dato objeto de la vulneración de segundad contendrá lo señalado en el artículo 43 de esta ley.	**Artículo 40, que refiere a la aplicación de una norma ISO de seguridad**

LOPDP	Reglamento de la ley No 29733, Ley de Protección de Datos Personales
En caso de que el responsable del tratamiento de los datos personales no cumpliese oportunamente y de modo justificado con la notificación será sancionado conforme al régimen sancionatorio previsto en esta ley. La notificación oportuna de la violación por parte del responsable cíe tratamiento al titular y la ejecución oportuna de medidas de respuesta, serán consideradas atenuante de la infra	
Art. 55.- Transferencia o comunicación internacional de datos personales. – La Página 27 de 40 transferencia o comunicación internacional de datos personales será posible si se sujeta a lo previsto en el presente capítulo, la presente Ley o la normativa especializada en la materia, propendiendo siempre al efectivo ejercicio del derecho a la protección de datos personales.	**Artículo 24.- Flujo transfronterizo de datos personales**. Los flujos transfronterizos de datos personales serán posibles cuando el receptor o importador de los datos personales asuma las mismas obligaciones que corresponden al titular del banco de datos personales o responsable del tratamiento que como emisor o exportador transfirió los datos personales. De conformidad con el artículo 15 de la Ley, además de los supuestos previstos en el primer y tercer párrafo de dicho artículo, lo dispuesto en el segundo párrafo dl mismo tampoco aplica cuando se traten de datos personales que deriven de una relación científica o profesional del titular y sean necesarios para su desarrollo o cumplimiento. **Artículo 25.- Formalización del flujo transfronterizo de datos personales**. Para los efectos del artículo precedente, el emisor o exportador podrá valerse de cláusulas contractuales u otros instrumentos jurídicos en los que se establezcan cuando menos las mismas obligaciones a las que se encuentra sujeto, así como las condiciones en las que el titular consintió el tratamiento de sus datos personales. **Artículo 26.- Participación de la Dirección General de Protección de Datos Personales respecto del flujo transfronterizo de datos personales.** Los titulares del banco de datos personales o responsables del tratamiento, podrán solicitar la opinión de la Dirección General de Protección de Datos Personales respecto a si el flujo transfronterizo de datos personales que realiza o realizará cumple con lo dispuesto por la Ley y el presente reglamento. En cualquier caso, el flujo transfronterizo de datos personales se pondrá en conocimiento de la Dirección General de Protección de Datos Personales, incluyendo la información que se requiere para la transferencia de datos personales y el registro de banco de datos.

LOPDP	Reglamento de la ley No 29733, Ley de Protección de Datos Personales
Art. 56.- Transferencia o comunicación internacional de datos personales a países **declarados como nivel adecuado de protección. –** Por principio general se podrán transferir o comunicar datos personales a países, organizaciones y personas jurídicas en general que brinden niveles adecuados de protección, y que se ajusten a la obligación de cumplimiento y garantía de estándares reconocidos internacionalmente conforme a los criterios establecidos en el Reglamento a la ley. Cuando resulte necesario por la naturaleza de la transferencia, la Autoridad dé Protección de Datos Personales podrá implementar métodos de control ex post que serán definidos en el Reglamento a la Ley. También establecerá acciones conjuntas entre las autoridades de ambos países con el objeto de prevenir, corregir o mitigar el tratamiento indebido de datos en ambos países. Para declarar de nivel adecuado de protección a países u organizaciones, la Autoridad de Protección de Datos Personales emitirá resolución motivada, en la que se establezca que la transferencia o comunicación internacional de datos personales cumple niveles adecuados de protección o de garantías adecuadas de protección, conforme a lo establecido en esta ley y su reglamento.	**Artículo 24., articulo 25, artículo 26 ya descritos**
Art. 57.- Transferencia o comunicación mediante garantías adecuadas. - En caso de realizar una transferencia internacional de datos a un país, organización o territorio económico internacional que no haya sido calificado por la Autoridad de Protección de Datos de tener un nivel adecuado de protección, se podrá realizar la referida transferencia internacional siempre que el responsable o encargado del tratamiento de datos personales ofrezca garantías adecuadas para el titular, para lo cual se deberá observar lo siguiente: a. Garantizar el cumplimiento de principios, derechos y obligaciones en el tratamiento de datos personales en un estándar igual o mayor a la normativa ecuatoriana vigente. b. Efectiva tutela del derecho a la protección de datos personales, a través de la disponibilidad permanente de acciones administrativas o judiciales; y,	**Artículo 24., articulo 25, artículo 26 ya descritos**

LOPDP	Reglamento de la ley No 29733, Ley de Protección de Datos Personales
c. El derecho a solicitar la reparación integral, de ser el caso. Para que ello ocurra, la transferencia internacional de datos personales se sustentará en un instrumento jurídico que contemple los estándares antes determinados, así como aquellos que establezca la Autoridad de Protección de Datos Personales, el mismo que deberá ser vinculante.	
Art. 59.- Autorización para transferencia internacional. Para todos aquellos casos no contemplados en los artículos precedentes, en los que se pretenda realizar una transferencia internacional de datos personales, se requerirá la autorización de la Autoridad de Protección de Datos, para lo cual, se deberá garantizar documentadamente el cumplimiento de la normativa vigente sobre protección de datos de carácter personal, según lo determinado en el Reglamento de aplicación a la presente Ley. Sin perjuicio de lo anterior la información sobre transferencias internacionales de datos personales deberá ser registradas previamente en el Registro Nacional de Protección de Datos Personales por parte del responsable del tratamiento o, en su caso, del encargado, según el procedimiento establecido en el Reglamento de aplicación a la presente Ley.	**Artículo 24., articulo 25, artículo 26 ya descritos**
Art. 60.- Casos excepcionales de transferencias o comunicaciones internacionales. - Sin perjuicio de lo establecido en los artículos precedentes se podrá realizar transferencias o comunicaciones internacionales de datos personales, en los siguientes casos; 1. Cuando los datos personales sean requeridos para el cumplimiento de competencias institucionales, de conformidad con la normativa aplicable; 2. Cuando el titular haya otorgado su consentimiento explícito a la transferencia o comunicación propuesta, tras haber sido informado de los posibles riesgos para él de dichas transferencias o comunicaciones internación a íes, debido a la ausencia de una resolución de nivel adecuado de protección y de garantías adecuadas. 3. Cuando la transferencia internacional tenga como finalidad el cumplimiento de una obligación legal o regulatoria; 4. Cuando la transferencia internacional de datos personales sea necesaria para la ejecución de un contrate entre el titular y el responsable del	**Artículo 24., articulo 25, artículo 26 ya descritos**

LOPDP	Reglamento de la ley No 29733, Ley de Protección de Datos Personales
tratamiento de datos personales, o para la ejecución de medidas de carácter precontractual adoptadas a solicitud del titular; 5. Cuando la transferencia sea necesaria por razones de interés público. 6. Cuando la transferencia internacional sea necesaria para la colaboración judicial internacional. 7. Cuando la transferencia internacional sea necesaria para la cooperación dentro de la investigación de infracciones 8. Cuando la transferencia internacional es necesaria para el cumplimiento dé compromisos adquiridos en procesos de cooperación internacional entre Estados; 9. Cuando se realicen transferencias de datos en operaciones bancarias y bursátiles. 10. Cuando la transferencia internacional de datos personales sea necesaria para la formulación, el ejercicio o la defensa de reclamaciones, acciones administrativas o jurisdiccionales y recursos; y, 11. Cuando la transferencia internacional de datos personales sea necesaria para proteger los intereses vitales del interesado o de otras personas, cuando el interesado esté física o jurídicamente incapacitado para dar su consentimiento,	
Art. 61.- Control continuo. - La Autoridad de Protección de Datos Personales en acciones conjuntas con la academia, realizará reportes continuos sobre la realidad internacional en materia de protección de datos personales. Dichos estudios servirán como elemento de control continuo del nivel adecuado de protección de datos personales de los países u organizaciones que ostenten tal reconocimiento. En caso de detectarse que un país u organización ya no cumple con un nivel adecuado de protección conforme los principios, derechos y obligaciones desarrollados en la presente Ley, la Autoridad de Protección de Datos Personales procederá a emitir la correspondiente resolución de no adecuación, a partir de la cual no procederán transferencias de datos personales, salvo que operen otros mecanismos de transferencia conforme lo dispuesto en el presente capítulo.	**Artículo 75.- Visita de fiscalización.** Para mejor resolver, se podrá ordenar a la Dirección de Supervisión y Control la realización de una visita de fiscalización, que se efectuará conforme a lo previsto en los artículos 108 a 114 del presente reglamento, dentro de los cinco (5) días siguientes de recibida la orden.

La Autoridad de Protección de Datos Personales publicará en cualquier medio, de forma permanente y debidamente la lista de países, organizaciones, empresas o grupos económicos que garanticen niveles adecuados de protección de datos personales

Art. 63.- Actuaciones previas. - La Autoridad de Protección de Datos Personales podrá iniciar, de oficio o a petición del titular, actuaciones previas con el fin de conocer las circunstancias de] caso concreto o la conveniencia o no de iniciar el procedimiento, para lo cual se estará conforme a las disposiciones del Código Orgánico Administrativo

Art. 64.- Procedimiento administrativo. - En el caso de que el responsable del tratamiento no conteste el requerimiento, en el término establecido en la presente ley, o éste fuere negado, el titular podrá presentar el correspondiente reclamo administrativo ante la Autoridad de Protección de Datos Personales, para lo cual se deberá estar conforme al procedimiento establecido en el Código Orgánico Administrativo, la presente ley y demás normativa emitida por la Autoridad de Protección de Datos Personales. Sin perjuicio, el titular podrá presentar acciones civiles, penales o constitucionales de las que se crea asistido.

Capítulo I

Disposiciones generales

Artículo 47.- Carácter personal.

Los derechos de información, acceso, rectificación, cancelación, oposición y tratamiento objetivo de datos personales sólo pueden ser ejercidos por el titular de datos personales, sin perjuicio de las normas que regulan la representación.

Artículo 48.- Ejercicio de los derechos del titular de datos personales.

El ejercicio de alguno o algunos de los derechos no excluye la posibilidad de ejercer alguno o algunos de los otros, ni puede ser entendido como requisito previo para el ejercicio de cualquiera de ellos.

Artículo 49.- Legitimidad para ejercer los derechos.

El ejercicio de los derechos contenidos en el presente título se realiza:

1. Por el titular de datos personales, acreditando su identidad y presentando copia del Documento Nacional de Identidad o documento equivalente.

El empleo de la firma digital conforme a la normatividad vigente, sustituye la presentación del Documento Nacional de Identidad y su copia.

2. Mediante representante legal acreditado como tal.

3. Mediante representante expresamente facultado para el ejercicio del derecho, adjuntando la copia de su Documento Nacional de Identidad o documento equivalente, y del título que acredite la representación.

Cuando el titular del banco de datos personales sea una entidad pública, podrá acreditarse la representación por cualquier medio válido en derecho que deje constancia fi dedigna, conforme al artículo 115 de la Ley Nº 27444, Ley del Procedimiento Administrativo General.

4. En caso se opte por el procedimiento señalado en el artículo 51 del presente reglamento, la acreditación de la identidad del titular se sujetará a lo dispuesto en dicha disposición.

Artículo 50.- Requisitos de la solicitud.

El ejercicio de los derechos se lleva a cabo mediante solicitud dirigida al titular del banco de datos personales o responsable del tratamiento, la misma que contendrá

1. Nombres y apellidos del titular del derecho y acreditación de los mismos, y en su caso de su representante conforme al artículo precedente.

2. Petición concreta que da lugar a la solicitud.

3. Domicilio, o dirección que puede ser electrónica, a efectos de las notificaciones que correspondan.

4. Fecha y firma del solicitante.

5. Documentos que sustenten la petición, de ser el caso.

6. Pago de la contraprestación, tratándose de entidades públicas siempre que lo tengan previsto en sus procedimientos de fecha anterior a la vigencia del presente reglamento.

Artículo 51.- Servicios de atención al público.

Cuando el titular del banco de datos personales o responsable del tratamiento disponga de servicios de cualquier naturaleza para la atención a su público o el ejercicio de reclamaciones relacionadas con el servicio prestado o productos ofertados, podrá también atender las solicitudes para el ejercicio de los derechos comprendidos en el presente título a través de dichos servicios, siempre que los plazos no sean mayores a los establecidos en el presente reglamento.

En este caso, la identidad del titular de datos personales se considera acreditada por los medios establecidos por el titular del banco de datos personales o responsable del tratamiento para la identificación de aquél, siempre que se acredite la misma, conforme a la naturaleza de la prestación del servicio o producto ofertado.

Artículo 52.- Recepción y subsanación de la petición.

Deben ser recibidas todas las solicitudes presentadas, dejándose constancia de su recepción por parte del titular del banco de datos personales o responsable del tratamiento. En caso de que la solicitud no cumpla con los requisitos señalados en el artículo anterior, el titular del banco de datos personales o responsable de su tratamiento, en un plazo de cinco (5) días, contado desde el día siguiente de la recepción de la solicitud, formula las observaciones por incumplimiento que o puedan ser salvadas de oficio, invitando al titular a subsanarlas dentro de un plazo máximo de cinco (5) días.

Transcurrido el plazo señalado sin que ocurra la subsanación se tendrá por no presentada la solicitud.

Las entidades públicas aplican el artículo 126 de la Ley Nº 27444, Ley del Procedimiento Administrativo General, sobre observaciones a la documentación presentada.

Artículo 53.- Facilidades para el ejercicio del derecho.

El titular del banco de datos personales o responsable del tratamiento está obligado a establecer un procedimiento sencillo para el ejercicio de los derechos. Sin perjuicio de lo señalado e independientemente de los medios o mecanismos que la Ley y el presente

reglamento establezcan para el ejercicio de los derechos correspondientes al titular de datos personales, el titular del banco de datos personales o el responsable del tratamiento, podrá ofrecer mecanismos que faciliten el ejercicio de tales derechos en beneficio del titular de datos personales.

Para efectos de la contraprestación que debe abonar el titular de datos personales para el ejercicio de sus derechos ante la administración pública se estará a lo dispuesto en el primer párrafo del artículo 26 de la Ley.

El ejercicio por el titular de datos personales de sus derechos ante los bancos de datos personales de administración privada será de carácter gratuito, salvo lo establecido en normas especiales de la materia. En ningún caso el ejercicio de estos derechos implicará ingreso adicional para el titular del banco de datos personales o responsable del tratamiento ante el cual se ejercen.

No se podrá establecer como medios para el ejercicio de los derechos ninguno que implique el cobro de una tarifa adicional al solicitante o cualquier otro medio que suponga un costo excesivo.

Artículo 54.- Forma de la respuesta.

El titular del banco de datos personales o responsable del tratamiento deberá dar respuesta a la solicitud en la forma y plazo establecido en el presente reglamento, con independencia de que figuren o no datos personales del titular de los mismos en los bancos de datos personales que administre.

La respuesta al titular de datos personales deberá referirse únicamente a aquellos datos que específicamente se hayan indicado en su solicitud y deberá presentarse en forma clara, legible, comprensible y de fácil acceso.

En caso de ser necesario el empleo de claves o códigos, deberán proporcionarse los significados correspondientes.

Corresponderá al titular del banco de datos personales o responsable del tratamiento la prueba del cumplimiento del deber de respuesta, debiendo conservar los medios para hacerlo. Lo señalado será de aplicación, en loque fuera pertinente, para acreditar la realización de lo establecido en el segundo párrafo del artículo 20 de la Ley.

Artículo 55.- Plazos de respuesta.

1. El plazo máximo de respuesta del titular del banco de datos personales o responsable del tratamiento ante el ejercicio del derecho de información será de ocho (08) días contados desde el día siguiente de la presentación de la solicitud correspondiente.

2. El plazo máximo para la respuesta del titular del banco de datos personales o responsable del tratamiento ante el ejercicio del derecho de acceso será de veinte (20) días

contados desde el día siguiente de la presentación de la solicitud por el titular de datos personales.

Si la solicitud fuera estimada y el titular del banco de datos personales o responsable del tratamiento no acompañase a su respuesta la información solicitada, el acceso será efectivo dentro de los diez (10) días siguientes a dicha respuesta.

3. Tratándose del ejercicio de los otros derechos como los de rectificación, cancelación u oposición, el plazo máximo de respuesta del titular del banco de datos personales o responsable del tratamiento será de diez (10) días contados desde el día siguiente de la presentación de la solicitud correspondiente.

Artículo 56.- Requerimiento de información adicional.

En el caso que la información proporcionada en la solicitud sea insuficiente o errónea de forma que no permite su atención, el titular del banco de datos personales podrá requerir dentro de los siete (7) días siguientes de recibida la solicitud, documentación adicional al titular de los datos personales para atenderla.

En un plazo de diez (10) días de recibido el requerimiento, contado desde el día siguiente de la recepción del mismo, el titular de datos personales

acompañará la documentación adicional que estime pertinente para fundamentar su solicitud. En caso contrario, se tendrá por no presentada dicha solicitud.

Artículo 57.- Ampliación de los plazos.

Salvo el plazo establecido para el ejercicio del derecho de información, los plazos que correspondan para la respuesta o la atención de los demás derechos, podrán ser ampliados una sola vez, y por un plazo igual, como máximo, siempre y cuando las circunstancias lo justifiquen.

La justificación de la ampliación del plazo deberá comunicarse al titular del dato personal dentro del plazo que se pretenda ampliar.

Artículo 58.- Aplicación de legislación específica.

Cuando las disposiciones aplicables a determinados bancos de datos personales conforme a la legislación especial que los regule establezcan un procedimiento específico para el ejercicio de los derechos regulados en el presente título, serán de aplicación las mismas en cuanto ofrezcan iguales o mayores garantías al titular de los datos personales y no contravengan lo dispuesto en la Ley y el presente reglamento.

Artículo 59.- Denegación parcial o total ante el ejercicio de un derecho.

LOPDP	Reglamento de la ley No 29733, Ley de Protección de Datos Personales
Art. 62.- Requerimiento directo del titular del dato de carácter personal al responsable del tratamiento. - El titular podrá en cualquier momento, de forma gratuita, por medios físicos o digitales puestos a su disposición por parte del responsable del tratamiento de los datos personales, presentar requerimientos, peticiones, quejas o reclamaciones directamente al responsable del tratamiento, relacionadas con el ejercicio de sus derechos, la aplicación de principios y el cumplimiento de obligaciones por parte del responsable del tratamiento., que tengan relación con él. Presentado el requerimiento ante el responsable este contará con un término de diez (10) días para contestar afirmativa o negativamente, notificar y ejecutar lo que corresponda.	La respuesta total o parcialmente negativa por parte del titular del banco de datos personales o del responsable del tratamiento ante la solicitud de un derecho del titular de datos personales, debe estar debidamente justificada y debe señalar el derecho que le asiste al mismo para recurrir ante la Dirección General de Protección de Datos Personales en vía de reclamación, en los términos del artículo 24 de la Ley y del presente reglamento. **Los descrito anteriormente**. Título IV Capítulo I Disposiciones Generales Artículos 47,48,49, 50, 51, 52, 53,54, 55, 56, 57, 58, 59

Nota. La tabla contiene una revisión artículo por artículo entre LOPDP de Ecuador con el Reglamento de la ley No 29733, Ley de Protección de Datos Personales del Perú.